NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DATA SUPPORTING MOBILE APPLICATION DEVELOPMENT FOR USE WITHIN THE MARINE AIR-GROUND TASK FORCE

by

Jesse D. Adkison

September 2015

Thesis Advisor:	John Gibson
Co-Advisor:	Charles Prince
Second Reader:	Douglas J. MacKinnon

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704–0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
DATA SUPPORTING MOBILE APPLICATION DEVELOPMENT FOR USE WITHIN THE MARINE AIR-GROUND TASK FORCE

5. FUNDING NUMBERS

6. AUTHOR Adkison, Jesse D.

7. PERFORMING ORGANIZATION NAME AND ADDRESS
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME AND ADDRESS
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE
A

13. ABSTRACT (maximum 200 words)

The United States Marine Corps has identified a need to provide handheld devices to allow operators to conduct wireless command and control-related functions. To fulfill this need, the Marine Corps initiated a program that aims at providing secure cellular communication capabilities down to the individual Marine to address gaps in existing command and control systems. Common wireless communication technologies that are typical within the average enterprise entity, such as text, email, and file sharing, among many others, do not exist on an individual level within the Marine Corps.

One of the next steps in advancing the implementation of handheld devices is to map requirements for information exchange to mobile device applications. This thesis accomplishes this mapping and identifies the application space where trusted devices offer the greatest potential for benefit to the Marines of the Major Subordinate Elements. While a suite of approved applications for military use may become available in the future, the initial applications for trusted devices can accomplish the needs for many users, thereby maximizing the utility of these devices in the short term.

14. SUBJECT TERMS
mobile device, mobile application, Marine Corps, Information Exchange Requirements, Marine Air-Ground Task Force, trusted handheld, IER, MAGTF, TH2

15. NUMBER OF PAGES
99

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01-280-5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DATA SUPPORTING MOBILE APPLICATION DEVELOPMENT FOR USE WITHIN THE MARINE AIR-GROUND TASK FORCE

Jesse D. Adkison
Captain, United States Marine Corps
B.S., Embry-Riddle Aeronautical University, 2008

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
September 2015

Author: Jesse D. Adkison

Approved by: John Gibson
Thesis Advisor

Charles Prince
Co-Advisor

Douglas J. MacKinnon, Ph.D.
Second Reader

Dan Boger, Ph.D.
Dean, Graduate School of Operations and Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The United States Marine Corps has identified a need to provide handheld devices to allow operators to conduct wireless command and control-related functions. To fulfill this need, the Marine Corps initiated a program that aims at providing secure cellular communication capabilities down to the individual Marine to address gaps in existing command and control systems. Common wireless communication technologies that are typical within the average enterprise entity, such as text, email, and file sharing, among many others, do not exist on an individual level within the Marine Corps.

One of the next steps in advancing the implementation of handheld devices is to map requirements for information exchange to mobile device applications. This thesis accomplishes this mapping and identifies the application space where trusted devices offer the greatest potential for benefit to the Marines of the Major Subordinate Elements. While a suite of approved applications for military use may become available in the future, the initial applications for trusted devices can accomplish the needs for many users, thereby maximizing the utility of these devices in the short term.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

3G	third generation
4G	fourth generation
AAR	after action report
AFRICOM	United States Africa command
ACE	air combat element
ARG	amphibious ready group
BFT	blue force tracker
BYOD	bring your own device
C2	command and control
CAS	close air support
CASEVAC	casualty evacuation
CCIR	commander's critical information requirements
CDD	Capabilities Development Directorate
CD&I	Combat Development and Integration
CE	command element
CENTCOM	United States central command
CEOI	communications-electronics operating instructions
CFF	call for fire
CIO	chief information officer(s)
CLR	combat logistics regiment
CMD	commercial mobile device
COIN	counterinsurgency
CONUS	continental United States
COP	common operation picture
COTS	commercial off-the-shelf
CTP	common tactical picture
DACAS	digitally aided close air support
DF	decision factor
DISA	Defense Information Systems Agency
DOD	department of defense
DPS	defense planning scenario
DPSS	digital precision strike suite
EHR	electronic heath records
EMO	enhanced MAGTF operations
EURCOM	United States European command

GCC	geographic combatant commander
GCE	ground combat element
GIG	global information grid
GPS	global positioning system
GRF	global response force
GRG	gridded reference graphic
HELP	handheld emergency logistics program
HIPAA	health insurance portability and accountability act
HVD	hosted virtual desktop
I&L	Installations and logistics
IER	information exchange requirement
IFF	identification friend or foe
INTREP	intelligence report
IP	Internet protocol
ISIMC	information security and identity management committee
IR	infrared
IT	information technology
IW	information warfare
JFC	joint force commander
JTF	joint task force
KILSWITCH	kinetic integration low-cost software individual tactical combat handheld
LCE	logistics combat element
LCpl	lance corporal
LTE	long-term evolution
LZ	landing zone
MAC	media access control
MADF	mobile applications development framework
MAG	Marine aircraft group
MAGTF	Marine air-ground task force
MarDiv	Marine division
MARFORCOM	U.S. Marine forces command
MAS	mobile application store
MAW	Marine aircraft wing
MC	mission critical
MCDP	Marine Corps doctrinal publication
MCRP	Marine Corps reference publication
MDM	mobile device management
MEB	Marine expeditionary brigade

MEDEVAC	medical evacuation
MEF	Marine expeditionary force
MEU	Marine expeditionary unit
MHG	MEF headquarters group
MLG	Marine logistics group
MOC	Marine Corps operating concepts
MSE	major subordinate element
MTTT	mobile technology tiger team
NCA	national command authority
NFC	near field communications
NMC	not mission critical
NSD	national security directive
OCR	optical character recognition
OS	operating system
PACOM	United States Pacific command
PC	personal computer
PFC	private first class
PLI	position, location, and identification
Pvt	private
QR	quick response
ROE	rules of engagement
ROMO	range of military operations
SA	situational awareness
SITREP	situation report
SME	subject matter expert
SMF	secure mobile framework
SOP	standard operating procedure
SPMAGTF	special purpose MAGTF
SPOTREP	spot report
USMC	United States Marine Corps
USMCCP	United States Marine Corps concepts and programs
VDI	virtual desktop interface
WO	warning order

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

The Marine Corps has not implemented a comprehensive mobile computing technology program, which has forced deployed Marines to function without the expediencies of modern communication standards. Personal mobile devices have become the standard for use in many large organizations, to the point of where their lack of employment is often regarded as a constraint. Part of the challenge of adopting mobile technology for battlefield use is identifying applications that will be used on these devices. To that end, principal information requirements need to be identified to satisfy the majority of the demands that will be placed on the mobile computing device. This research conducts an analysis of existing information exchange requirements within the functional elements of the Marine Corps Air/Ground Task Force (MAGTF) to derive those communication events that are most critical to the development and adoption of applications for mobile devices.

B. PURPOSE

The purpose of this research is to evaluate critical information exchange requirements within the MAGTF and to determine the type of applications that would be the most effective for individual Marines to use on a handheld device when engaged in deployed operations.

C. RESEARCH QUESTIONS

This research aims to answer the following questions:

1. How are the communications and information exchange needs within the MAGTF evaluated to reflect maximum usability to the largest population of users?
2. What applications on a trusted device will be the most pertinent to the largest population of users within the MAGTF?

3. What are the occasions that users can use a trusted device to meet communication and information exchange needs?

D. OBJECTIVES

Given the recent demand for Department of Defense (DOD) components to begin evaluating mobile applications for inclusion into the Mobile Application Store (MAS) (Bernhart-Walker, 2014; CIO Council, 2012b), attention should be paid to the specific applications that will benefit the widest variety of Marines and their associated mission sets. The objective of this research is to isolate and identify the unique mobile device applications on which the Marine Corps should place developmental emphasis.

E. METHODOLOGY

A comprehensive data set of end-user Information Exchange Requirements (IERs), which were identified and produced by the Capabilities Development Directorate, will first be evaluated using cross-matrix analysis to narrow down the communication events that are commonly used. Next, the most prolific and widely used individual IERs, as they pertain to each functional element within the Marine Corps, will be placed into an additional matrix to determine if the same IER could be a viable candidate for mobile application development. In the second matrix, a variety of factors that are associated with mobile application applicability will be used to rate the IER as to its overall suitability for application development. Those factors will be compiled and assimilated to determine the most widely needed trusted device applications.

F. SCOPE

This research will be limited to those particular IERs that are commonly communicated at the Marine Corps Company level and below. This organizational level restriction is useful as it applies to all three functional elements of the Marine Corps and restricts the data to manageable levels. Furthermore, Marine Corps doctrine specifically focuses efforts to address Company level operations (Conway, 2008a, 2008b; USMC, 2014b).

G. THESIS ORGANIZATION

This thesis is organized around a thorough background, two-part analysis, and a practical conclusion. Characterized as individual chapters, these sections will provide supporting and relevant data to produce a short list of candidates for future use.

Chapter II provides background regarding the organization and use of the Marine Corps and how it operates. It introduces competencies later associated with the data derived by the Capabilities Development Directorate. Smart phone use and adoption is discussed to support the hypothesis that mobile device usage is on the rise. The chapter shows mobile device usage and familiarity is increasing with users that are of military age. Adoption within enterprise level organizations is researched in order to provide relevance as well as a link to DOD practices that are currently in place. Federal, DOD, and USMC policies are introduced to show that mobile device usage is being deliberated and policies are being put in place to govern the use and implementation of future mobile device use.

In Chapter III, commercially available mobile applications are introduced as enterprise and military examples of the types of applications that currently exist. This also functions to display the plethora of information that may be gathered using organic built-in tools on modern smart phones. Finally, the IERs derived by the Capabilities Development Directorate are introduced and discussed.

Chapter IV provides more detail with respect to the rationale and analysis of the IER data. Here, the data are screened and narrowed down to a finite list that will satisfy analysis requirements. That data are further analyzed to determine practical applications that are needed for the Marine Corps. Using a matrix to measure application applicability across 10 decision factors, a ranked list of IERs is produced.

Chapter V summarizes the data found in Chapter III and presents it with conclusions. This chapter presents the most relevant IERs that should be

considered for development and inclusion into the Mobile Application Store. It specifically discusses possible attributes that could be associated with the most viable IERs as well as discussing the potential reasoning as to why some IERs were not viewed as having the highest potential for development.

II. GOVERNMENTAL MOBILE DEVICE POLICIES, PLANS, AND PROCEDURES

A. THE MARINE AIR-GROUND TASK FORCE

The United States Marine Corps (USMC) shapes its forces into scalable organizations called Marine Air-Ground Task Forces (MAGTFs). These are balanced combined-arms forces that are unified under a single commander (USMC, 1998, 2013b). All MAGTFs are composed of four elements: a Command Element (CE), a Ground Combat Element (GCE), an Air Combat Element (ACE), and a Logistics Combat Element (LCE) (see Figure 1) (Conway, 2006; USMC, 2010). The CE is the Task Force's Headquarters unit. It delivers the Command and Control (C2), direction, and planning capabilities to the Force (USMC, 1998). The GCE contains the infantry, armor, artillery, reconnaissance, and engineer forces necessary to carry out the mission of the MAGTF (USMC, 1998). The ACE is a task-organized composite aviation unit that is reinforced with subordinate elements needed to carry out the six functions of Marine aviation, with the primary purpose of supporting the ground forces (USMC, 1998). Finally, the LCE is the element within the MAGTF that is responsible for providing Combat Service Support (USMC, 1998).

The MAGTF is a forward deployed element of national power that carries out the missions of the National Command Authority (NCA), Geographic Combatant Commanders (GCC), and Joint Force Commanders (JFC) (Eldridge, 2013). After more than a decade of operating in a campaign-centric manner of warfare, the Marine Corps is in the process of returning to its amphibious roots by positioning itself as what the 35th Commandant, General James Amos (2012), calls "a middleweight force from the sea" (p. 7). The venerable MAGTF is this middleweight force that is scalable in terms of both size and capability (Amos, 2012).

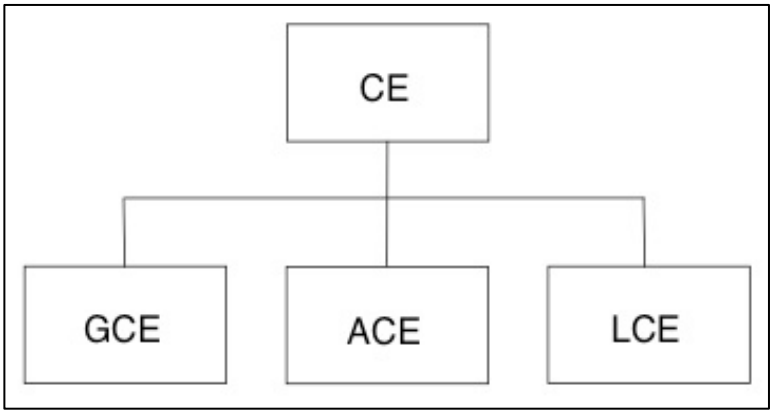

Figure 1. MAGTF Organization (after USMC, 1998)

1. Types of MAGTFs

The Marine Corps' combined arms force is further organized into four major types of MAGTFs. These MAGTFs maintain the four core elements as depicted in Figure 1 but are tailored to meet specific mission requirements. The four types of MAGTFs are the Marine Expeditionary Force (MEF), the Marine Expeditionary Brigade (MEB), the Marine Expeditionary Unit (MEU), and the Special Purpose MAGTF (SPMAGTF) (Conway, 2008b; USMC, 1998).

The Marine Corps Reference Publication (MCRP) 5–12D (1998) states that the largest type of MAGTF, the Marine Expeditionary Force (MEF), is the principle Marine Corps warfighting organization (p. 2–2). The three standing MEFs employ approximately 35,000 to 55,000 Marines and Sailors and are capable of conducting a wide range of military operations (ROMO) in any geographic environment (Conway, 2008b). This self-sustaining force comprises combat elements that consist of a MEF Headquarters Group (MHG), a Marine Division (MarDiv), a Marine Aircraft Wing (MAW), and a Marine Logistics Group (MLG) (USMC, 1998, 2014b).

As set forth in Expeditionary Force 21, the capstone concept that guides the future of the Marine Corps, the MEF will undergo organizational restructuring aimed at streamlining the force while maintaining support of the national strategy (USMC, 2014b). I MEF will continue to maintain the nation's requirement for a

Global Response Force (GRF) that is ready, trained, and equipped to respond to crises around the world (USMC, 2014b). As the nation shifts its focus to the Asia-Pacific area, III MEF will maintain a focus within the U.S. Pacific Command (PACOM) by functioning as a Joint Task Force (JTF) headquarters (Amos, 2012; USMC, 2014b). The II MEF CE will merge with U.S. Marine Forces Command (MARFORCOM) in an effort to reduce the number of headquarters units within the Marine Corps while still maintaining its posture as a GRF (USMC, 2014b).

The Marine Expeditionary Brigade is a highly scalable organization that is capable of executing operations across the ROMO as well as functioning as the lead element of a JTF headquarters (Conway, 2008b; USMC, 2014b). Smaller than a MEF and larger than a MEU, the theoretical MEB is structured around a reinforced infantry regiment, a composite Marine Aircraft Group (MAG), and a Combat Logistics Regiment (CLR) (Conway, 2008b). One of the most appealing aspects of the MEB is the Command Element's ability to 'composite forward' to rapidly form a cohesive MAGTF that is flexible in size and scope (USMC, 2014b). Under Expeditionary Force 21, the standing MEBs CEs will nest within their geographical MEF and will also be aligned with their respective MEF's regional focus and mission. First and 2nd MEB will align with I and II MEF, respectively (USMC, 2014b). As such, 1st MEB will be regionally oriented on U.S. Central Command (CENTCOM) and 2nd MEB will orient on U.S. Africa Command (AFRICOM) and U.S. European Command (EUCOM) (see Figure 2) (USMC, 2014b).

Figure 2. MEB Regional Orientation (from USMC, 2014b)

The Marine Expeditionary Unit is the smallest and most responsive type of MAGTF. As a forward-deployed extension of the MEF, the MEU provides approximately 2,500 Marines for immediate reaction to crises throughout the globe (Conway, 2008b). The MEU is composed of one of seven individual standing CEs, a reinforced infantry battalion, a reinforced composite squadron, and a combat logistics battalion (Conway, 2008b; USMC, 1998). While embarked on a Navy Amphibious Ready Group (ARG) or operating disaggregated, the MEU is capable of providing limited combat operations, build-up actions for follow-on forces, or contingency operations. Both of the continental United States (CONUS) MEFs provide three standing CEs. One CE will be stood up to form an operational MEU at any given time. III MEF maintains the 31st MEU, the only continuously forward-deployed MEU (USMC, 2014a). The MEU is the Marine Corps' principle contribution to the GRF mission (USMC, 2014b).

The Special Purpose MAGTF is a force that is specifically tailored to address the GCC's specific needs. While scalable, the SPMAGTF is normally not larger than a MEU and maintains the four core elements organic to a MAGTF (USMC, 1998). The SPMAGTF is typically designed to conduct security

cooperation exercises, to gain regional familiarity or to position forces in anticipation of developing crises (USMC, 2014b).

2. MAGTF's Range of Military Operations

The MAGTF is a flexible, task-organized force that is capable of conducting multiple, diverse, and simultaneous range of missions (USMC, 2010). While the ROMO for various MAGTFs is large and varied, we will present three missions that demonstrate the variety of operating environments that Marines experience: power projection, crisis response, and small wars. These missions comprise the Defense Planning Scenarios (DPS) that will be used as a measure of variety for the Marines in a deployed MAGTF environment (Capabilities Development Directorate, 2012).

Power projection is a capability of a nation to extend its influence to distant shores by a variety of means. The third edition of the Marine Corps Operating Concepts (MOC) defines power projection as

> The ability of a nation to apply all or some of its elements of national power—political, economic, informational, or military—to rapidly and effectively deploy and sustain forces in and from multiple dispersed locations to respond to crises, to contribute to deterrence, and to enhance regional stability. (p. 90)

Air power and sea power are the two broad categories by which the United States projects military influence (USMC, 2010). Sea power provides the versatility, access, lethality, and means to project national power on a much larger and more sustainable scale (USMC, 2010). The Marine Corps is the principle military force that is organized to project sea power into the littoral environments. Understanding power projection is central to the concept of how the Marine Corps operates and why it is of primary importance when evaluating the use of equipment that Marines may utilize.

Crisis response is the national reaction to a rapidly developing threat to the United States or its interests that produces a circumstance such that the commitment of military forces and/or resources is considered to accomplish

national objectives (DOD, 2014). The Marine Corps is poised to respond to a range of global crises quickly. General Amos refers to this mindset in Expeditionary Force 21 as being "expeditionary" in nature—to be able to deploy and arrive quickly and to begin operating immediately upon arrival (p. 6). Any evaluation of tools that may aid a Marine in his or her mission must consider this ethos.

Small wars, otherwise known as counterinsurgency (COIN) operations or information warfare (IW), is defined in the MOC as:

> Operations undertaken under executive authority, wherein military force is applied—usually in combination with the other elements of power—in the internal or external affairs of another state whose government is unstable, inadequate, or unsatisfactory for the preservation of life and of such other interests as are determined by the foreign policy of our Nation. (p. 11)

Small wars is a historical term used to describe irregular warfare and low-intensity conflicts (USMC, 1940). The 1940 publishing of the *Small Wars Manual* is evidence of the regularity of irregular warfare in our Nation's past. Recent history has shown that low-intensity conflicts continue now and will continue to occur into the future. The Marines' ability to operate in austere environments, otherwise known as "Small Wars ruggedness" (USMC, 2010), is also determinative in developing a matrix for evaluating use of equipment.

The three planning scenarios described above have been selected as metrics to cover the width and breadth of MAGTF operations. The power projection, crisis response, and small wars scenarios will be used as a backdrop to evaluate the individual communication requirements within all three combat elements of the Marine Air-Ground Task Force.

B. SMARTPHONE ADOPTION

A smartphone is a type of mobile device that possesses features such as a touchscreen display, wireless Internet access, position location, as well as the ability to run additional user-selected applications. Mobile devices, including

tablets, are designed to offer the conveniences of computers in a more portable format (USMC, 2013a). The Department of Defense and Marine Corps describe the mobile device as:

> A handheld computing device with a display screen that allows for user input. When connected to a network, it enables the sharing of information in formats specially designed to maximize the use of information given device limitations. (USMC, 2013a)

The number of people, particularly Americans, using smartphones is rising. According to ABI Research, there will be over more than 7.4 billion mobile devices by 2015 (Ericom, 2012). This prediction is validated by ACI's 2014 measure that there are 7.7 billion mobile devices in the world—more than the number of humans on Earth (Gunelius, 2014). The ABI research also suggests that another 1.2 billion smartphones will be added over the next five years (Ericom, 2012). In 2011, the number of smartphone shipments surpassed the number of personal computer (PC) shipments. From 2011 to 2012, the number of Americans that owned smartphones rose by 11% (CIO Council, 2012a). The U.S. government also expects that by 2015, more Americans will access the Internet by mobile devices than by PCs (CIO Council, 2012a). In the third quarter of 2012, Apple shipped 17 million iPad tablets, which represents an 84% growth over the previous year (Ericom, 2012).

In 2013, the Pew Research Center published its findings on the growing trend in smartphone ownership. Of the 91% of Americans that own cellular phones, 61% of them state that they own a smartphone (Smith, 2013). As seen in Figure 3, this result reveals that over one-half of Americans now own smartphones (Smith, 2013).

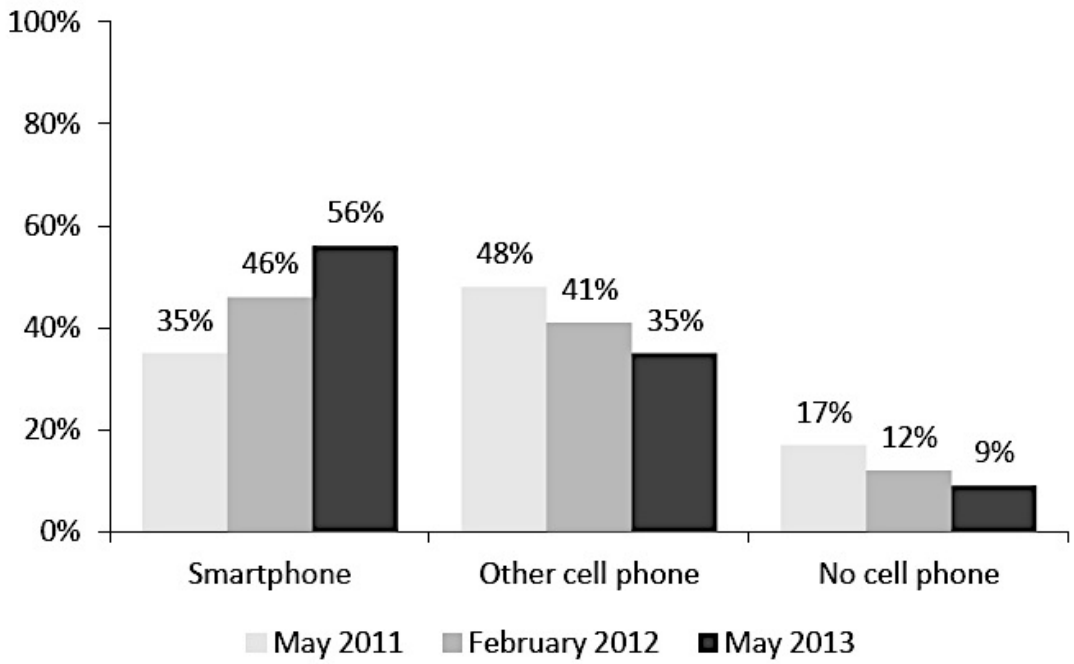

Figure 3. Changes in U.S. Adult smartphone ownership (after Smith, 2013)

From 2011 to 2013, every major demographic group demonstrated growth in smartphone adoption including age, race, and education level (Smith, 2013). Gender had little effect on ownership with 59% of men adopting smartphone technology versus 53% of women (Smith, 2013). Young adults showed a particular attraction to smartphone ownership despite varying income levels (see Figure 4) (Smith, 2013). This indicates that the ownership rates of 18–29 and 30–49 age demographics could translate into similar figures for those Americans that are in the military due to corresponding age spectrums (Mercado & Murphy, 2011; USMC, 2012).

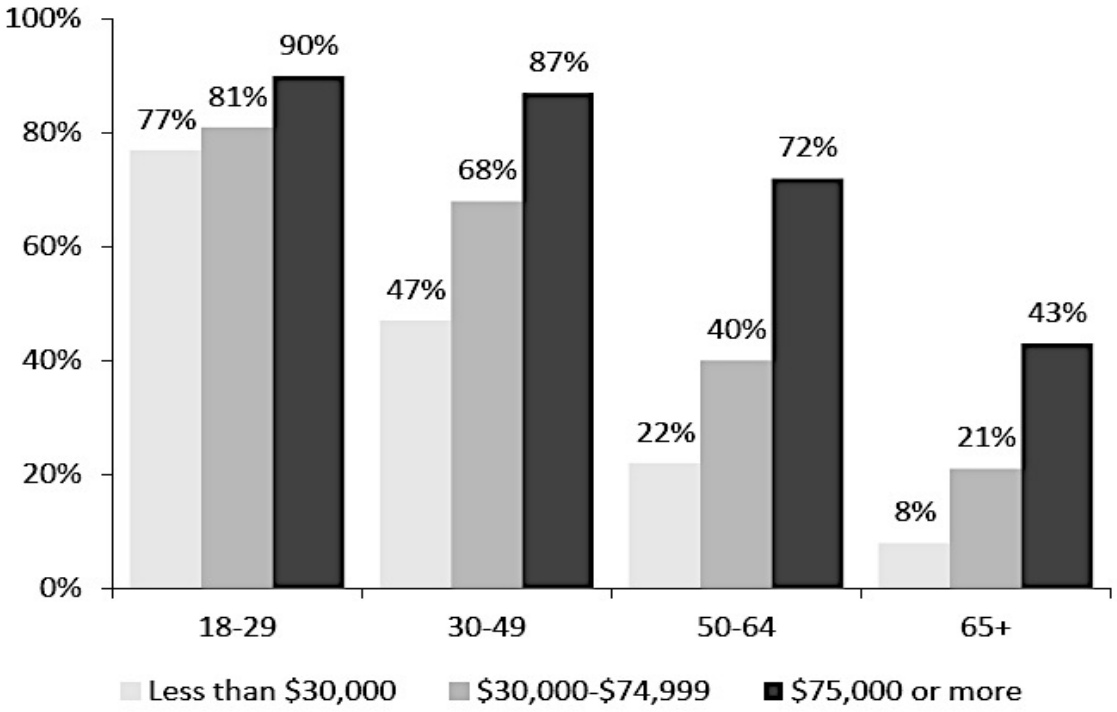

Figure 4. Smartphone Ownership by Income & Age
(after Smith, 2013)

The December 2012 USMC Demographics Update showed that the Marine Corps is by far the most junior of all of the services. Forty-one percent of Marines are Lance Corporals (LCpl), Privates First Class (PFC), or Privates (Pvt). The majority of Marines with the rank of E-1 through E-3 are 29 or fewer years old. This is significant compared to the next closest service in the category, the U.S. Navy, which has 23% of its Sailors at the rank of E-3 or below (USMC, 2012). The Demographics Update also indicated that only 7% of Marines are women (p. 11) and that 62% of the entire USMC is 25 years of age or younger (p. 2). When compared against American adult smartphone adoption statistics from Smith's study and given the above demographic data, it is reasonable to infer that a large population of the United States Marine Corps is young and has most likely adopted smartphone technology.

The United States Army also appears to have experienced similar mobile device adoption rates among its soldiers. A 2011 study by Mercado and Murphy

titled *Evaluating Mobile Device Usage in the Army* reported most soldiers own a mobile device of some sort (p. 1). While 79% of all soldiers reported owning a mobile device, 94% of soldiers under the age of 20 have adopted mobile technology (Mercado & Murphy, 2011). Furthermore, those soldiers who do own smartphones use them habitually (Mercado & Murphy, 2011).

While the vast majority of young Americans, Marines, and soldiers own more mobile devices than older generations, additional studies show that one age demographic does not necessarily demonstrate a proclivity to use the smart features of the device more than another age demographic (Gafni & Geri, 2013). Gafni and Geri's 2013 study shows that length of ownership determines usage (p. 21). Those who have owned their smartphones longer tend to access the Internet by mobile device more frequently than they would if a computer were nearby and available (Gafni & Geri, 2013).

C. ENTERPRISE MOBILE DEVICE POLICIES AND PROGRAMS

Recent studies have shown that as much as 60% of employees within enterprise level organizations regularly use their devices at work. Additionally, some organizations have also reported that 75% of the devices on their networks are employee owned (Extreme Networks, 2014). Although information technology (IT) managers and departments within larger organizations have largely adopted policies that support mobile technologies such as bring your own device (BYOD) programs, the DOD and, more particularly, the Marine Corps has taken a more protracted approach (CIO Council, 2012b; Good Technology, 2011).

1. Enterprise Mobile Device History

The history of mobile device policies is linked to the evolution of smartphones. As cellular telephones and wireless technologies advanced, policies and practices governing their authorized use and integration progressed as well. Early smartphones, such as the BlackBerry, were able to connect to the

Internet and they became the phone of choice for many due to their ability to send and receive email (Ericom, 2012). The introduction and subsequent growth of Apple's iPhone piloted a new era of smartphone users that were eager to integrate their iPhone with their work as they had done in their personal life. Competition among mobile device manufacturers has further introduced additional technologies and form factors, such as the tablet, that drive the demand for mobile device integration within enterprise systems (Ericom, 2012).

2. Benefits of Mobile Device Programs

Organizations incorporating policies that embrace the use of mobile devices benefit by experiencing increased productivity, cost savings, and flexibility/mobility in terms of value derived from organizational goals and objectives (Nah, Siau, & Sheng, 2005). The Federal CIO's Council stated that "the use of mobile technology provides opportunities for innovation, agility and flexibility in the workplace." (CIO Council, 2012b). Generally, users are more productive when they are able to accomplish tasks on familiar devices (Ericom, 2012).

Realizing cost savings can be controversial. For example, Ericom (2012) believes that in allowing users to utilize their own mobile devices, large organizations can avoid increased costs that can be associated with equipping users with rapidly evolving mobile technologies. Gartner (2011) counters with the assertion that mobile device integration programs are rarely associated with cost savings and that equipment costs only account for around 20% of the total cost of ownership of the device (p. 2).

The debate over whether or not mobile device integration programs result in cost savings differs just as widely as the practices that are put into place. Cost associated options in BYOD policies range from full coverage of the devices and support being borne by the organization to policies that require employees to purchase, update, and maintain their mobile devices (Good Technology, 2011). Around one-half of the companies that are implementing BYOD policies opt to

allow their employees to bear all of the cost associated with working on their own mobile devices (Good Technology, 2011). Although this notion may be counter-intuitive, research has shown that non-subsidized employees would rather pay to use devices of their choice (Good Technology, 2011; Pearlson & Saunders, 2012). Another option that many organizations are adopting is the practice of subsidizing the use of employee devices through a reimbursement program. This proves to be a popular choice as employee satisfaction increases when they are able to use their own devices, upon management approval. (Good Technology, 2011).

Not surprisingly, companies that choose to integrate mobile devices into their IT infrastructure frequently experience higher percentages of employee flexibility and mobility (Pearlson & Saunders, 2012). Good Technology (2011) reports that organizations that support BYOD programs experience a 12% increase in employee mobility (p. 10). This increase in mobility can have real worth for organizations, such as the Marine Corps, who value mobility as an objective (Nah et al., 2005; USMC, 2014b). Real advantages can be attained as a result of implementing mobile device integration programs; however, there are significant obstacles to their adoption as well.

3. Challenges to Implementing Mobile Device Programs

The adoption of mobile device policies presents a significant challenge to not only the IT department, but management as well. BYOD integration inevitably leads to more devices within the network, which presents many potential problems. Ericom (2012) identifies the likely trouble areas that IT departments will need to address:

- **Security –** The use of personal devices within the enterprise network introduces vulnerabilities because of the increased number of devices that are difficult to secure individually.
- **Compliance –** The adherence to regulations specific to each organization, such as Health Insurance Portability and Accountability Act (HIPAA) standards and other National Security

Directives (NSD) (DISA, 2013) become increasingly difficult to administer with mobile users.

- **Management –** Along with the variety of mobile devices and their varying operating systems (OS) and form factors comes the responsibility of ensuring that all devices are maintained with the most up-to-date anti-virus, connection brokers, and proprietary software.
- **Support –** Increasing the number of individual end devices will inevitably result in a proportionate increase in trouble calls. This will tax IT help desks tremendously as they will be expected to identify and implement solutions across a range of mobile devices (Ericom, 2012).

All of the difficulties listed above unavoidably lead to increased costs. These challenges place an increased load upon already overextended IT staffs. The additional burden on IT resources will be a source of significant cost increases (Ericom, 2012). However, many companies are now offering mobile device management (MDM) and virtual desktop interface (VDI) software packages that ease the transition into a mobile friendly work environment. This makes the management and support concerns more palatable to IT managers. Organizational managers that are apprehensive about security and compliance are coming to terms with the fact that mobile device programs are becoming increasingly popular with larger companies that have significant informational breaching concerns. Good Technology (2011) reports that larger organizations within sectors that are information-driven, such as financial services and healthcare, have the most to gain from implementing mobile device policies (p. 6). The Marine Corps is just such an organization.

4. Mobile Device Needs within Large Organizations

One of the biggest challenges faced by large organizations integrating mobile devices within their networks is balancing the wants and expectations of the end users with the organization's goal of managing risk and costs (Wallin, 2011). Studies have shown that users will frequently use personal devices within organizational networks with or without approval from IT departments (Extreme

Networks, 2014). Users anticipate a device agnostic, (Dixon, 2012) comprehensive personal security package that is completely transparent with regard to ease of integrating with networks. They further expect an experience that mirrors the quality of service that they would normally have at home (Extreme Networks, 2014).

Given the desire of users to integrate personal devices within organizational networks, managers must implement programs that automate onboarding, profiling, securing, managing, and troubleshooting such devices (Extreme Networks, 2014; Pearlson & Saunders, 2012). The process of onboarding include the mechanisms that IT departments use to identify, authenticate, and, initially, provide the user with mobile device policy acceptance—all with minimal input from the user (Aruba Networks, 2014). Profiling is procedures used to determine which users and what equipment is on the network. It is, essentially, the registration of a user and his or her device with many attributes such as, but not limited to (Extreme Networks, 2014):

- Device type
- Manufacturer
- Media access control (MAC) address
- Internet Protocol (IP) address
- Hostname
- Username
- OS – with version number
- Current physical location
- Communications protocol
- Access point or service set identifier
- Switch or port
- Phone number
- First or last time seen
- Applied policy

Profiling provides the essential information to assign access to a level of detail that is in accordance with the organization's mobile device policy. Managing and troubleshooting devices on the network is commonly accomplished through the use of two methods of control: MDM and VDI or hosted virtual desktop (HVD) software (Ericom, 2012; Extreme Networks, 2014). MDM solutions protect data and configuration settings on mobile devices and are typically supplied through third-party vendors (Extreme Networks, 2014). Using information attained through the profiling process, MDM software controls access to applications and data through wireless management of the mobile device's configuration based on user access level and permissions (Wallin, 2011). VDI and HVD products protect the location of essential and protected data by limiting access via thin-client or zero-client solutions (Ericom, 2012; Extreme Networks, 2014). Together, these products and solutions provide a comprehensive answer to many IT and corporate managerial concerns confronting the integration of mobile technologies within the modern agile work force.

5. Implementing Mobile Device Programs

Integrating a mobile device plan into an existing organization can be complicated and requires a focus on a number of key areas. The development of corporate policies is a first step toward arriving at a contract that supports the needs of both the organization and the end users. These policies should address issues such as user and device eligibility, device ownership, access to corporate data and resources, as well as security and privacy obligations (Wallin, 2011).

The contract between users and the organization must attend to a variety of concerns that protect both parties and should be completed in writing. Wallin (2011) asserts that written acceptance of organizational policy is more visible and apparent to users as opposed to a simple click-through acknowledgment on individual devices (p. 2). A number of matters can be attended to and are considered to be best practices. Users should be responsible to secure and back-up any and all personal content on the device and, in the case of corporate

owned devices, maintain the device. They should be made aware that, as a result of MDM programs and other organization policies, the user experience could be detrimentally affected. Many MDM programs also monitor and restrict user's activity and access. Employees need to be aware of how the organization uses and secures this information. In addition, users must acknowledge that they may be required to turn over their device for findings and discovery. Finally, users may be asked to sign an anti-litigation clause that could limit their ability to sue the organization in the event of infringement of the mobile device policies (Wallin, 2011). Of course, all of these concerns will need to be in alignment with appropriate laws within individual states and countries as well as the organization's human resources department.

Organizations must adopt practices that classify user and device eligibility. A risk matrix based on location, user background, and sensitivity of information being accessed or generated, among other factors, may be applied to stratify or categorize the users into access levels (Wallin, 2011). This user segmentation will need to be modified on an individual basis. Device selection and eligibility can be evaluated according to varying levels of detail. Minimum device requirements, such as performance and memory capabilities, may be enforced in order to accomplish tasks. Not all devices are able to accomplish all tasks, resulting in the exclusion of particular form factors in certain cases (Wallin, 2011). Despite the widely accepted policy of device agnostic mobile programs (Ericom, 2012), organizations may choose to limit access to portions or all of its network based on OS or manufacturer (Extreme Networks, 2014). These classification practices are managed by the MDM and will support the organization's effort to provide a secure and manageable mobile device policy.

Device ownership and associated costs must also be factored into mobile device programs. As previously noted, a range of methods may be employed to deal with costs related to mobile device use. However, reimbursement programs have been shown to encourage mobile device usage and integration (Good Technology, 2011). Basic reimbursement practices include the compensation for

the device itself and/or costs linked to voice, messaging, and data plans. More detailed policies may consider private versus organizational uses as well as placing a cap on either compensation as a whole, as in a stipend, or limiting expense-back programs to certain mobile categories such as data usage (Good Technology, 2011).

Wallin (2011) further identifies cost related items for attention in *Gartner's View on 'Bring Your Own' in Client Computing*. These considerations could include:

- Tax liabilities associated with stipends and whether or not they are treated as salary or non-taxable income
- The replacement policy for lost, stolen, or damaged devices as well as the necessity to immediately report the loss, theft, or belief that the mobile device has been compromised.
- How or whether the assorted applications, services, and accessories used with the device are reimbursed.
- A plan relating to how the user can replace, upgrade, or add an additional device to the program.
- Compensation for varying cloud-based services (p. 3).

6. Mobile Device Implementation Conclusion

While costs of devices, programs and policies, and the accompanying monetary risk associated with implementing a BYOD program can appear daunting and complicated, research has shown that most end users simply want to use their personally owned device at work (Good Technology, 2011; Pearlson & Saunders, 2012). Large organizations that seek to integrate mobile devices into their networks and business practices must take this and the previously mentioned factors into consideration. Organizations would like to increase productivity and employee satisfaction while maintaining security and low costs. End users would like to utilize the device of their choosing while knowing that their private information will be kept secure. Most prominent among their requirements is ease of use—both in accessing the network and enjoying a high quality user experience. A policy that balances these matters will precede an

effective mobile device implementation strategy. What is clear is that large organizations must be proactive in seeking a strategy that works for them in order to maintain employee productivity and satisfaction, competiveness, and compliance in a time that is growing more and more agile (Good Technology, 2011; Pearlson & Saunders, 2012).

D. FEDERAL, DOD, AND USMC MOBILE DEVICE POLICIES AND PROGRAMS

The United States government is adapting to the ubiquitous transformation in which its citizens place an increasing demand on mobility and access to the digital domain. This demand presents an immediate challenge (CIO Council, 2012b). Departments and agencies within the government architecture are adhering to policies and guidance that are vertically aligned to support the integration of mobile devices in order to satisfy demand and confront mission needs.

1. Federal Mobile Device Guidance

In 2012, the U.S. government developed a strategy entitled *Digital Government: Building a 21st Century Platform to Better Serve the American People.* This plan seeks to build upon existing and emerging digital technologies and focus various initiatives in order to "increase return on IT investments; reduce waste and duplication; and to increase the effectiveness of IT solutions" (CIO Council, 2012a, p. 3). In line with previously noted enterprise efforts, the federal government views the integration of IT solutions, including mobile devices, as both an opportunity and a complex undertaking (CIO Council, 2012a). The main thrust of the government's efforts in the digital realm is to coordinate and focus the design and modernization of the Federal IT infrastructure to ensure future interoperability, privacy, and security (CIO Council, 2012a).

a. Digital Government Strategy Objectives and Principles

The federal government's ambitions to integrate information systems involve three objectives. The first objective is to facilitate high-speed access to government data at anytime, anyplace, and on any device (CIO Council, 2012a). This objective aims to modify the way the government structures its model to deliver information and services in a manner that is device agnostic (CIO Council, 2012a). The next effort is to be procedurally and fiscally responsible in the procurement and management of devices, applications, and data. This resolution guides the change in how the government presents data. It is moving away from merely placing existing data online and gravitating toward structuring the information to exist within the global information grid (GIG) from the beginning (CIO Council, 2012a). The third objective is to enable American innovation and education through straightforward access to governmental information (CIO Council, 2012a).

Three approaches have been developed to accomplish these objectives. An information-centric approach will be used to modernize the way data are handled. In this manner, content is thought of as specific pieces of information rather than digitized documents (CIO Council, 2012a). A shared approach is coordinating efforts to streamline and standardize digital practices across governmental agencies (CIO Council, 2012a). A customer-centric approach guides the delivery and presentation of information to the public in a manner of the people's choosing (CIO Council, 2012a). These three approaches are enveloped in an overarching principle of security and privacy to ensure the safe and private use and access to government information and services (CIO Council, 2012a).

Specific milestones have been developed to manage the Digital Government Strategy. Milestone 10.2 is of particular interest to this research as it specifies the federal government's direction to integrate the use of mobile devices. This milestone calls for the evaluation of "opportunities to accelerate the

secure adoption of mobile technologies into the Federal environment at reduced costs" (CIO Council, 2012a, p. 2, 2012b, p. 25).

b. Government Use of Mobile Technology Implementation Analysis

In response to milestone 10.2 of the Digital Government Strategy, the Federal CIO Council directed the Information Security and Identity Management Committee (ISIMC) to assemble a Mobile Technology Tiger Team (MTTT) to research the adoption of mobile technologies (CIO Council, 2012b). The MTTT's conclusions are in the form of recommendations in areas to focus further research to successfully adopt mobile devices within the federal government.

The first among five total recommendations is to define the requirements for an MDM policy and a Mobile Application Store (MAS) with reference to specific use cases (CIO Council, 2012b). This recommendation directly relates to this research in that it reinforces the importance of organizations to select mission-related use cases to evaluate their mobile device needs before entering into the procurement process. This organization-specific process sets the baseline upon which future decisions can be based. This research draws from the MTTT's first recommendation as a directive to distill the efforts of the U.S. Marine Corps in pursuing the most desirable applications that are relative to its diverse mission.

2. Department of Defense Mobile Device Guidance and Policy

The Department of Defense Mobile Device strategy is nested within the federal government's guidance. This plan is ensconced within and promulgated by Joint Force 2020. Joint Force 2020 is the capstone concept for joint operations as identified by the Chairman of the Joint Chiefs of Staff. It specifically identifies mobile technology as the key enabler in the concept of globally integrated operations (Dempsey, 2012). Behind the globally integrated operations concept is the idea that networked forces will need to become more fluid and more proficient across all domains and geographic obstacles

(Dempsey, 2012). A principal tenet to this idea is that the integration of mobile devices will provide for networked operations by equipping distributed forces to access information and collaborate in real time (Dempsey, 2012).

Directly addressing the integration of mobile devices within the DOD is the CIO's Commercial Mobile Device (CMD) Implementation Plan. This guidance is an update to the DOD's Mobile Device Strategy and it should be noted that this policy is non-tactical in nature (DISA, 2013). However, it does demonstrate the DOD's commitment and desire to integrate mobile devices into the DOD infrastructure; that integration into tactical environments may not be too distant. The CMD Implementation Plan provides the structure and policies necessary to foment the development and evolution of the DOD's information architecture to support mobile devices, initiate mobile device policies, and guide the maturation and utilization of mobile applications (DISA, 2013). Among the many policies and guidelines that are set forth in this implementation plan is the mobile applications framework, which pilots the development of defense related mobile device applications.

The CMD Implementation Plan identifies two sets of guidelines for mobile applications. First is the requirement for a mobile application storage and distribution center that is a direct action resulting from the federal government's MAS recommendation (DISA, 2013). Applications that are stored there will be certified through a vetting process before inclusion into the application storage center (DISA, 2013). The other demand calls for the mobile application development framework to be established (DISA, 2013). This standards-based framework is to be compatible with all OSs, leverage commercial off-the-shelf (COTS) technology, while remaining within security and compliance regulations (DISA, 2013). The DOD's CMD implementation plan also directs component level CIOs with mobile application related tasks such as:

- Provide a list of approved CMD applications
- Provide instructions on how to obtain the applications
- Provide descriptions of the application's function

- Make the applications available to the MAS
- Develop application management guidelines
- Ensure CMD applications processes conform to security standards (DISA, 2013, p. 14)

The Department of Defense recognizes that mobile devices, BYOD programs, and mobile application development and management are facets of an enduring IT trend (DISA, 2013). The DOD Principle Deputy CIO, Robert Carey, has even stated that "the dismounted soldier or Marine in Afghanistan has to have the same kinds of connectivity as someone working stateside" (Parsons, 2012). However, current policies, constructs, and vulnerabilities preclude the immediate inclusion of mobile technologies into the existing DOD infrastructure (DISA, 2013). The DOD CIO will continue to monitor developments within the mobile technology industry and accordingly generate policies needed to support BYOD integration (DISA, 2013).

3. United States Marine Corps Information Technology Guidance

Marine Corps Doctrinal Publication (MCDP) – 6, *Command and Control*, states that information is used for two purposes. One use is to generate situational awareness (SA) to support decision making. The other purpose is to manage the execution of that decision (Eldridge, 2013; USMC, 1996). The Marine Corps must address how to effectively deliver that information in austere environments, whenever the warfighter needs it (Nally, 2010). Mobile devices will expedite the distribution of that information (CIO Council, 2012a).

The 35th Commandant of the Marine Corps, General James Amos, broadly established the mindset that the USMC must equip its warfighters with new capabilities and technologies in order to confront unrest in some of the most contested and isolated parts of the world (see Figure 5) (Amos, 2010). He further expounded on these priorities when he promulgated the vision and plan for the future of the Marine Corps in *Expeditionary Force 21*. This document shapes the evolution of the Marine Corps into the 21st century. One of the focus areas

identified in the blueprint is the improvement in accessing and sharing information (USMC, 2014b). This advancement calls for the refinement in unclassified and secret network integration as well as improving the processing and distribution of real time tactical data (USMC, 2014b). It demands that distributed planning and operations become the norm as well as leveraging reach-back capabilities to access information, people, and tools to accomplish missions (USMC, 2014b).

Figure 5. Priorities of the 35th Commandant of the Marine Corps (from Amos, 2010)

The demand for increased access to information through the advancement of technology by isolated and distributed forces is fundamental to the concept of Enhanced MAGTF Operations (EMO) (USMC, 2010). As published in the third edition of the *Marine Corps Operating Concepts*, EMO draws upon improvements in technology and understanding to "push all elements of the MAGTF to become lighter, more adaptable, more resourceful, and faster in relation to the enemy" (USMC, 2010, p. 31). The key to achieving these aims is to become lighter (Amos, 2010; Conway, 2008b; Dixon, 2012; USMC, 2013b, 2014b). After a significant period of operating in a campaign of land style warfare in Iraq and Afghanistan, the USMC will need to undergo a paradigm shift by lightening the force and the individual. The *Marine Corps Operating Concepts* seeks to slim down the MAGTF by making use of emerging technologies in the effort to make every system smaller, lighter, and more efficient while reducing its

dependencies on vehicles (USMC, 2010). It also places load limits on the individual Marine. Marines will now be limited to assault loads of 75 pounds or less and existence loads that do not exceed 150 pounds (USMC, 2010). These requirements outline a force that is swift, light, and foot mobile. EMOs will be executed by Marines with considerable network connectivity who are not dependent on vehicle-mounted communications systems. To conform to these stipulations, this future MAGTF must utilize lightweight mobile technologies to accomplish their assigned missions in distributed and austere environments.

4. Marine Corps Information Technology Policies

In the spirit of supporting the EMO concept, Marine Corps C2 efforts are focused on the integration of warfighters, intelligence, actions, and supporting elements into a network-enabled distributed combat force (USMC, 2013b). Central to the development of the C2 portfolio is the determination of necessity regarding C2 capabilities (USMC, 2013b). The USMC (2013b) characterizes this approach as “desired versus required” capabilities (p. 23). This technique of concise selection during times of budgetary frugality produces difficult choices for C2 investment organizations. Procurement of C2 related systems must be carefully scrutinized in order to ensure that the required capabilities are being met.

Gap analysis of net-enabled capabilities has uncovered a number of command and control shortfalls. The required capabilities that the Marine Corps are seeking are in the areas of SA, common operational picture (COP), network capacity, target validation, and data management (USMC, 2013b). Situational awareness is commonly referred to as simply knowing what is occurring in one’s environment. However, in the C2 capacity, the USMC desires the ability to provide friendly position location down to the lowest level (USMC, 2013b). The COP is defined by the DOD (2014) as “a single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness” (p. 42). C2

planners would like to increase the accuracy and timeliness of the flow of information within the COP (USMC, 2013b). The network capacity shortfall is the inability to provide sufficient information transport capacity (USMC, 2013b). The throughput necessary to put these capabilities to use is not adequate at the tactical level. Developing the ability to conduct real-time targeting and target effects is another C2 shortfall (USMC, 2013b). Timeliness is a critical factor when employing effects-based targeting and the Marine Corps would like to conduct lethal and non-lethal fires in real time (DOD, 2002; USMC, 2013b). Finally, C2 leaders want to increase the availability to crucial data as well as how Marines access, fuse, disseminate, store, search, and retrieve that information (USMC, 2013b).

This set of specifically required capabilities are integral to the type of net-centric warfare that is the expectation of what lies ahead of the Marine Corps in the 21st century. A Marine Corps that is fiscally constrained while being scaled down in support of the EMO concept must still furnish these C2 essentials. Mobile technologies have the ability to address many, if not all, of these requirements. Mobile devices, once integrated, authenticated, and configured with fundamental applications, have the ability to dramatically increase SA and facilitate the COP while delivering access to information for targeting and decision-making.

Corresponding to the Federal Digital Government Strategy, DOD Mobile Device Strategy, and the Marine Corps Information Enterprise Strategy, the Marine Corps has developed a congruent model with its own unique characteristics. The Marine Corps Mobile Device Strategy (2013a) prescribes the way ahead for mobile devices within the USMC with four major objectives. These objectives are:

- “Establish a secure mobile framework (SMF).”
- “Collaborate with DOD and industry partners to develop a classified mobile device capability.”
- “Transition the unclassified mobile device infrastructure to a cost effective and platform agnostic environment.”

- "Incorporate personally owned mobile devices." (p. 3)

These objectives are consistent with previously referenced research from enterprise level civilian organizations as well as Federal and DOD directives. This published strategy indicates that the Marine Corps is committed to providing an agile method to access informational needs through the use of mobile devices (USMC, 2013a).

Of the objectives listed above, the objective of establishing an SMF is the most relevant to this research. The development of the SMF will ensure the appropriate parameters are determined to support USMC requirements prior to the procurement, testing, and fielding of mobile technologies (USMC, 2013a). One of the important aspects of the SMF is the development of secure mobile applications. The Marine Corps acknowledges that mobile applications can offer value and a near limitless range of possibilities and advantages but remain appreciably concerned with potential security risks associated with their use (Nah et al., 2005; USMC, 2013a). The Marine Corps is also committed to the common mobile application development processes as set forth by the DOD CIO's CMD Implementation Plan in order to ensure joint application interoperability (USMC, 2013a).

5. Impact on USMC Mobile Device Procurement and Application Development

The federal government, DOD, and USMC have all developed implementation plans, policies, procedures, and strategies that target the inclusion of mobile technologies within the overall government IT infrastructure. The preponderance of resources and dedication to this topic indicates that the incorporation of mobile devices is not a question of "if" it will occur but rather "when and how" it will occur. Government mobile device implementation strategies appear to mirror some of the best practices that are indicated by leading research groups. This suggests that while the DOD may not be keeping

pace with enterprise-leading, mobility-adaptive organizations, the department is proceeding accurately.

The Marine Corps is getting lighter and more agile while training and equipping its warfighters with some of the most innovative technology available. In the current climate of fiscal restraint, the USMC must be very fastidious in its provisioning of technologies. Basing much of the procurement process on the disposition of “desired versus required” necessitates investigation into precisely what capabilities fall into the category of required. The numerous capabilities that a mobile device possesses can be combined and utilized to produce a virtually endless supply of useful mobile applications (Nah et al., 2005). However, not all of these mobile applications may be uniquely required for the purposes of mission success as defined by the Marine Corps. The Marine Corps should know which types of applications would be of most relevant use across the ROMO within the MAGTF.

E. CHAPTER SUMMARY

This chapter reviewed the composition and mission of the MAGTF, including how it performs the three DPSs utilized in the IER analysis. The Marine Corps performs a specific service to the nation as a middleweight force in readiness (USMC, 2013b). Smartphones were identified, defined, and categorized by their demographic usage. Mobile devices are being used more frequently and their ownership and usage in the United States and among U. S. military personnel is increasing. The history of enterprise mobile device solutions was explored and the benefits and challenges of adopting mobile devices in the work environment explained. Examples of BYOD policies were examined and some best practices identified. Overall, mobile device usage is increasing and organizations will need to develop policies and procedures on how they will integrate with them.

Next, Federal, DOD, and USMC policies and guidance regarding mobile device adoption are examined. As a whole, the policies appear to be in alignment and present a nested approach to the mobile device adoption issue.

III. THE MOBILE DEVICE AND APPLICATION DOMAIN

Mobile devices come in a variety of sizes and form factors but the most common and popular of these platforms is the smartphone (Futuremark, 2014). According to *PC Magazine* (2014), a smartphone is

> a cellular telephone with built-in applications and Internet access. In addition to digital voice services, modern smartphones provide text messaging, email, Web browsing, still and video cameras, and digital music and video playback.

The modern smartphone has a range of features that are available to the user. Combinations of these features can be used in conjunction with third party developers to produce an endless variety of mobile applications (Downs et al., 2014).

Beyond the intrinsic cellular voice, text, email, and web access capabilities of a modern smartphone are a number of features that make the device even more valuable. One of the most visually striking characteristics that distinguishes a smartphone from an ordinary cellular phone is its large display screen. The large display screens on modern smartphones range from less than three to more than seven diagonal inches of viewing area (FindTheBest, 2014). The touchscreen display of most smartphones is not only the method of conveying information from the device to the user but also provides the interactive method of inputting data and controls (Downs et al., 2014). The touchscreen also offers varying keyboard configurations as well as fingertip gestures and, in some cases, stylus inputs.

Smartphones utilize a variety of wireless protocols that enable the device to connect and interact with a wide range of access points and other devices. In addition to standard third and fourth generation (3G and 4G) and Long Term Evolution (LTE) cellular technologies, many smartphones have the capability of integrating with other devices through additional wireless technologies. Wi-FI (IEEE 82.11-based wireless access) is the standard method in which all modern

smartphones and computers connect with wireless networks (TechTerms, 2014). Mobile hotspot tethering is the ability to either link two mobile devices together over a Wi-Fi connection or provide access to data services through a smartphone cellular provider (FindTheBest, 2014; Nadel, 2014). Bluetooth is a wireless standard that is used to exchange data over short distances between two or more Bluetooth enabled and paired devices (Bluetooth, 2014). It is used to wirelessly connect external devices such as headsets, sensors, and computers to a smartphone over short distances in order to interact with those devices. Infrared (IR) wireless technology is used in much the same way as a Bluetooth connection. IR communications suffer from line-of-sight issues but are routinely used to wirelessly control devices such as entertainment components, headsets, and modems. Near Field Communications (NFC) is an emerging wireless technology that exchanges data only at very close ranges, usually less than a few inches. Unlike Bluetooth, NFC does not require pairing and is being used as a wireless payment option for many retailers (Carter, 2013).

The image capturing capability that is universal among contemporary smartphones assists many mobile applications beyond simply recording an image for recollection (Downs et al., 2014). Digital cameras can also be used to interpret quick response (QR) codes, barcodes, and foreign languages; facilitate augmented reality; conduct visual searches; or function as a document scanner. The video recording capabilities within smartphones offer many additional capabilities along with the inclusion of sound. Microphones on smartphones have a myriad of uses as well including smartphone control, voice recording, and language translation.

Location services have completely changed the way smartphones are used. The inclusion of a global positioning system (GPS) receiver within a smartphone has not only transformed the phone into a navigation device, but has converted the smartphone into a sensor, tracker, and data collector. Position location alone enables a smartphone user to know where he or she is in relation to other entities in the environment and to use that information in support of or

conjunction with other features. Position location in combination with other data and applications makes the smartphone an even more useful tool (Downs et al., 2014). A GPS enabled device enables a subscriber to track nearly anything to which the device is attached. Position location has evolved from simple precision navigation to the integration with data that provides users with context-aware information relevant to their surroundings (Unhelkar & Murugesan, 2010). Precise position data, when collected, is also used to target users with statistical and marketing efforts.

Other smartphone features such as multi-axis accelerometers, compass, light sensors, and light emitters can provide an additional array of capabilities (Downs et al., 2014). The features that are organic to the modern smartphone make it a unique platform to carry out a variety of functions. However, the smartphone's real potential becomes apparent once these basic capabilities are utilized in concert with a mobile application.

A. MOBILE DEVICE APPLICATIONS

DISA (2013) singles out mobile device applications as "a critical enabler for service delivery and will permit new opportunities to improve mission effectiveness" (p. 4). Mobile applications that are specifically developed to address military needs can have a tremendous effect on individual SA as well as the overall COP. These military mobile applications combined with non-military utilities and organic smartphone technologies create a potent mobile capability that can address many of the shortfalls identified by the Marine Corps Command and Control Roadmap (USMC, 2013b).

1. Mobile Application Capabilities and Development

A number of mobile application taxonomies exist in order to differentiate their varying levels of complexity. These taxonomies provide categorization to mobile applications that can be useful in determining which types may be pertinent to an organization. A useful model of mobile application codification is

Unhelkar and Murugesan's New Taxonomy for Enterprise Mobile Applications (see Figure 6). A generalized military interpretation on this established framework can also be used to provide structure and classification to military mobile applications.

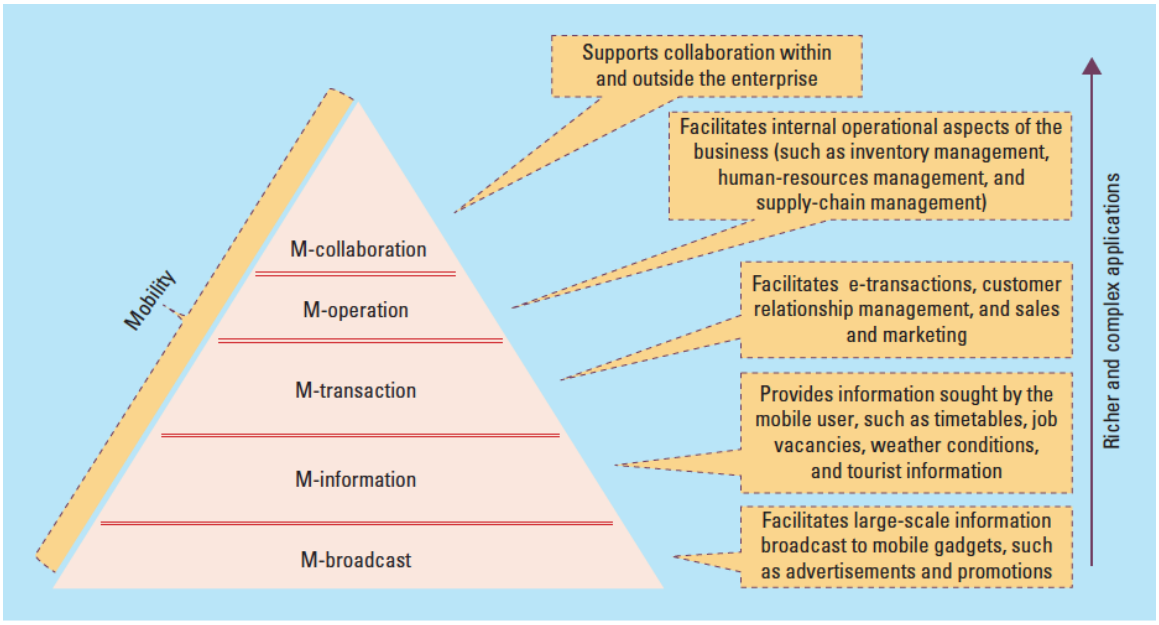

Figure 6. Unhelkar and Murugesan's taxonomy of mobile applications (from Unhelkar & Murugesan, 2010)

The classification is useful in the dissection of applications into categories of varying levels of complexity. It is also valuable to focus developer's efforts on the primary characteristics of mobile application design and execution (Unhelkar & Murugesan, 2010). Increasing in richness and complexity, the five categories of mobile applications are Broadcast, Information, Transaction, Operation, and Collaboration (Unhelkar & Murugesan, 2010). Military applications can be associated within these categories with the administration of appropriate security measures.

a. Mobile Broadcast

The Mobile Broadcast category is the most rudimentary type of application that simulcasts information to mobile devices. These applications reach large numbers of users within prescribed network boundaries due to the non-discriminatory nature of the message delivery architecture. Mobile Broadcast applications can be used as an early warning system for emergencies within cellular networks. They can also be employed to target users for marketing or other useful information such as sales specials, bus schedules, or cinema programs (Unhelkar & Murugesan, 2010). The military use for this type of application could include the circulation of general information such as friendly and known enemy locations, local weather and advisories, or other pertinent alerts or warnings.

b. Mobile Information

The Mobile Information category encompasses the class of applications that provide user-requested information. Enterprise and civilian uses for this variety of application are endless. Requests for information related to news, weather, sports, schedules, prices, products, and services are just a few of the multitude of areas that users often solicit (Unhelkar & Murugesan, 2010). The military implementation of the Mobile Information category is equally vast. Marines could arm themselves with information related to operating manuals and troubleshooting techniques, historical reports, or various database queries.

c. Mobile Transaction

The Mobile Transaction level represents an increased level of sophistication not found in the previous two categories. Transactional applications enable users to place, make payment on, and track orders for products and services. The higher order of performance required to facilitate transactions represents a development strategy that must address heightened security, faster responses, higher reliability, and increased trust within the application (Unhelkar & Murugesan, 2010). Retailer-developed electronic

payment applications such as the Starbucks iPhone application (see Figure 7), along with third-party providers such as PayPal, permit the possibility of secure mobile transactions. While the direct correlation to military applicability may not exist on a large scale, the increased security and performance parameters necessary for a mobile payment transaction represents a corresponding level of trust required for many military information transactions.

Figure 7. Starbucks iPhone payment application (from Starbucks, 2015)

d. Mobile Operation

Unhelkar & Murugesan's Mobile Operation category of applications includes a level of dynamic interaction not seen in the preceeding classifications. These advanced applications integrate personnel functions such as payroll, leave, and schedules as well as back-end business activities like inventory and

production schedules (Unhelkar & Murugesan, 2010). The dynamic nature of this type of application directly relates to the sort of functions that occur within military administration and operations departments. The production of daily flight schedules involve the cooperative interaction between aircraft maintenance, airfield operations, training, ordinance, and many other sections. Personnel administration centers rely on multiple databases to satisfy member's needs. Logistical units demand real time access to information in order to manage the availability of gear and supplies. The integration of these back-end systems enable mobile users to conveniently obtain information necessary to accomplish their missions.

e. Mobile Collaboration

The Mobile Collaboration category raises the level of dynamic interaction within the application. Multiple users can now work together in partnerships to accomplish the goals of the organization. Networking groups of applications also can be classified within this category. The dynamic cooperation among the various stakeholders along with associated databases and software modules create a complex style of application that is correspondingly difficult to construct (Unhelkar & Murugesan, 2010). The essence and inherent complexities related to military command and control offer an appropriate arena to develop these types of applications. The coordination necessary to exercise C2 in complex environments could be more manageable through Mobile Collaboration applications.

2. Development Challenges

One of the more demanding issues facing mobile application developers is the increasingly complex nature and pace of mobile device development. Current mobile users demand applications that function across all platforms and form factors. They would like to see applications that are location-aware, incorporate dynamic learning to provide user-relevant content, and provide a highly

interactive user experience (Unhelkar & Murugesan, 2010). These demands are made more difficult to fulfill with additional requirements and restrictions such as seamless and invisible security as well as battery and bandwidth limitations (Unhelkar & Murugesan, 2010). Mobile application development frameworks have been developed to help advance and deliver these increasingly sophisticated applications.

Extensive communications frameworks such as the Zachman Framework for Enterprise Architecture and The Open Group Architecture Framework have provided a foundational background for the relaying of complex ideas and organizational direction (Zachman International, 2014). The Mobile Application Development Framework (MADF) (see Figure 8) is a schema specifically developed to counter the myriad developmental challenges associated with mobile applications. The MADF provides an architecture and visual model that brings together concomitant layers that are useful in addressing mobile application issues. The MADF consists of five layers that address communications, information, middleware and binding, applications, and presentation. These layers are ensconced in an orthogonal security layer that applies to all areas (Unhelkar & Murugesan, 2010).

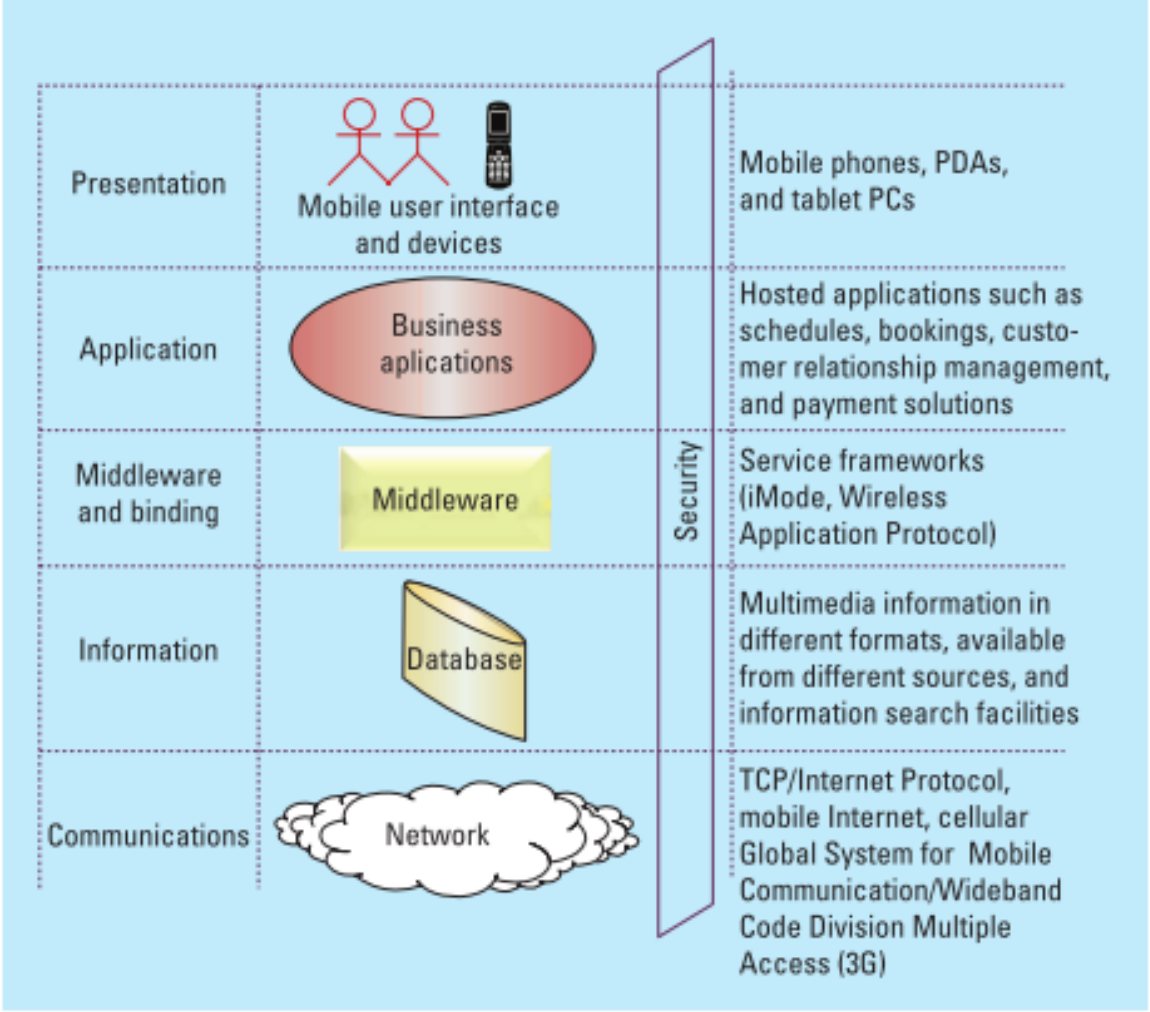

Figure 8. The Mobile Applications Development Framework (from Unhelkar & Murugesan, 2010).

The varying layers within the MADF contribute to the development process by supplying developers with areas on which to contemplate functionality and interoperability. The Communications layer provides the underlying infrastructure on which mobile telecommunications exists. Here, developers examine various wireless network and telecommunication standards and their effect on the other layers as well as the user's quality of service. The Information layer is the domain that addresses how information will be obtained and presented to the user. Multiple avenues of information delivery, such as text, graphical, audio, video, or any combination thereof, provide many opportunities

for mobile application developers to enhance the user's experience. The Middleware and Binding layer explores the method of connecting the application with actual content. Here, middleware protocols are used or developed to aid in the functionality of the application. Next, the Applications layer contains the business rules regarding how the organization will use the actual application. Finally, the Presentation layer addresses user interaction with the application. Screen size, user interaction and input, and profiling are all areas of consideration when providing the user with a positive and enhancing event (Unhelkar & Murugesan, 2010).

3. Enterprise Application Examples

As of June, 2014, the world's two leading application repositories, Apple's iOS App Store and Google's Google Play, each shelve approximately 1.2 million mobile device applications (Perez, 2014). With such an extensive array of available applications from which to choose, providing compelling examples to illustrate how applications can provide value to organizations is not difficult. However, the following applications were selected in an effort to counter the widespread phobia of mobile devices within the DOD (Parsons, 2012) with examples within industries that also require heightened levels of security and connectivity.

a. Aviation Application: ForeFlight Mobile

The ForeFlight Mobile Application is an aviation resource that is being promoted as a pilot's second-in-command. The application has many features that are useful to aviators both on the ground and in the air. When combined with external receivers, the iOS application provides location-aware data for airports, including runway information, operating hours, and frequencies. When linked with approved avionics packages, the application provides further interaction. For example, touching a frequency on an airport diagram or aviation map will change the aircraft's radios to match the selection. ForeFlight also offers on-the-move

access to over a dozen continually updated maps and charts that can be critical to flight safety. These digital publications also represent a considerable size and weight savings compared to conventional flight bags. Commensurate with the Mobile Operations category of complexity, ForeFlight Mobile's strengths lie within the integration of the applications parts. The blending of a selection of features can be illustrated by examining Figure 9.

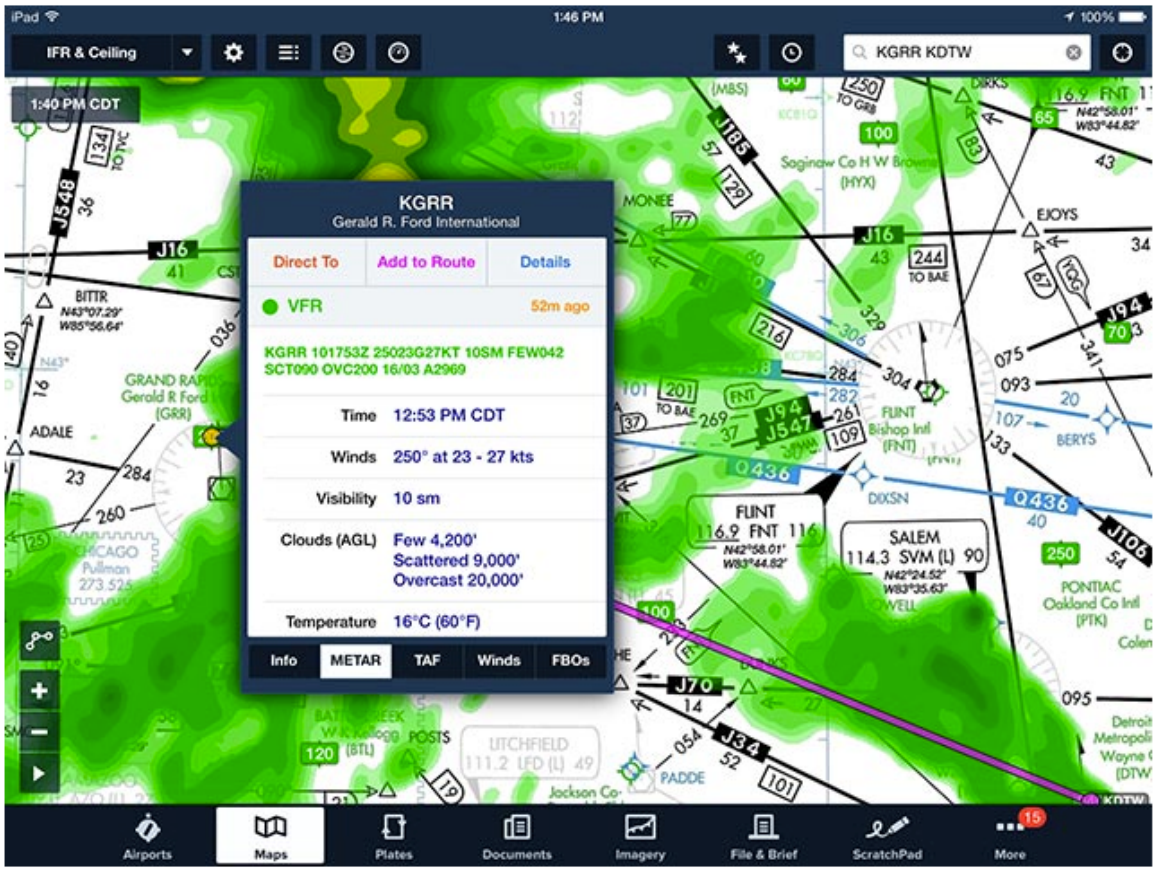

Figure 9. ForeFlight Mobile Screenshot (from ForeFlight, 2014)

The ForeFlight Mobile screenshot demonstrates the use of multiple resources that combine to provide pilots with an abundance of usable information. In the example, the purple line represents a pilot's flight plan. In this case, the path is overlaid on a high-altitude route chart that incorporates in-flight XM satellite weather graphics. The Gerald R. Ford International Airport is

selected and its associated information is displayed on an additional layer. From here, the pilot may add this airport to his or her flight plan, select frequencies to communicate with controllers at the airport, or find out if the airfield has the infrastructure to support this particular aircraft (ForeFlight, 2014). Without the ForeFlight Mobile application, this set of information would require multiple charts and communication events that may not constitute the most current information available. This aviation tool represents the type of mobile application that can be developed and implemented within a highly regulated industry that is extremely safety conscious and security aware. ForeFlight Mobile also represents a group of applications that could provide a basis for crossover to military use.

b. Healthcare Application: DrChrono

DrChrono is a mobile application that is one of the most popular and highest ranked healthcare tools within the e-health sector (Brown-Willson Group, 2014). It is a mobile Electronic Health Records (EHR) end-to-end management solution that represents the Mobile Collaboration level of applications with its sophisticated level of interoperability. At its core, DrChrono provides charting, scheduling services, and medical billing while interfacing with multiple users and databases (DrChrono, 2014). The Brown-Willson Group (2014) list the most basic of EHR systems employ functional components as “patient demographics, patient problem lists, electronic medication lists, clinical notes and documentation, order entry management of prescriptions, viewing capability of laboratory, and imaging results” (p. 8). They also identify, in addition to the basic components listed above, what a fully functioning EHR system should include such as “clinical notes and documentation of the medical history and follow-up, ordering of laboratory and radiology tests. electronic transmission of prescriptions and orders, and electronic return of images, clinical decision support with warnings of drug interactions or contraindications, highlighting of out-of-range test levels, and reminders regarding guideline-based interventions or screening.” (p. 8)

DrChrono integrates all of these functions and does so with a presentation that is user friendly (see Figure 10) and also incorporates one of the industry's most popular requests: speech-to-text functionality (Brown-Willson Group, 2014; TheAppMagazine, 2014). The EHR application allows multiple users to collaborate across time and space to provide the best patient care possible. DrChrono's ability to provide a noteworthy mobile application within a very highly regulated industry is evidence that mobile device implementation can be achieved within organizations with comparable security concerns.

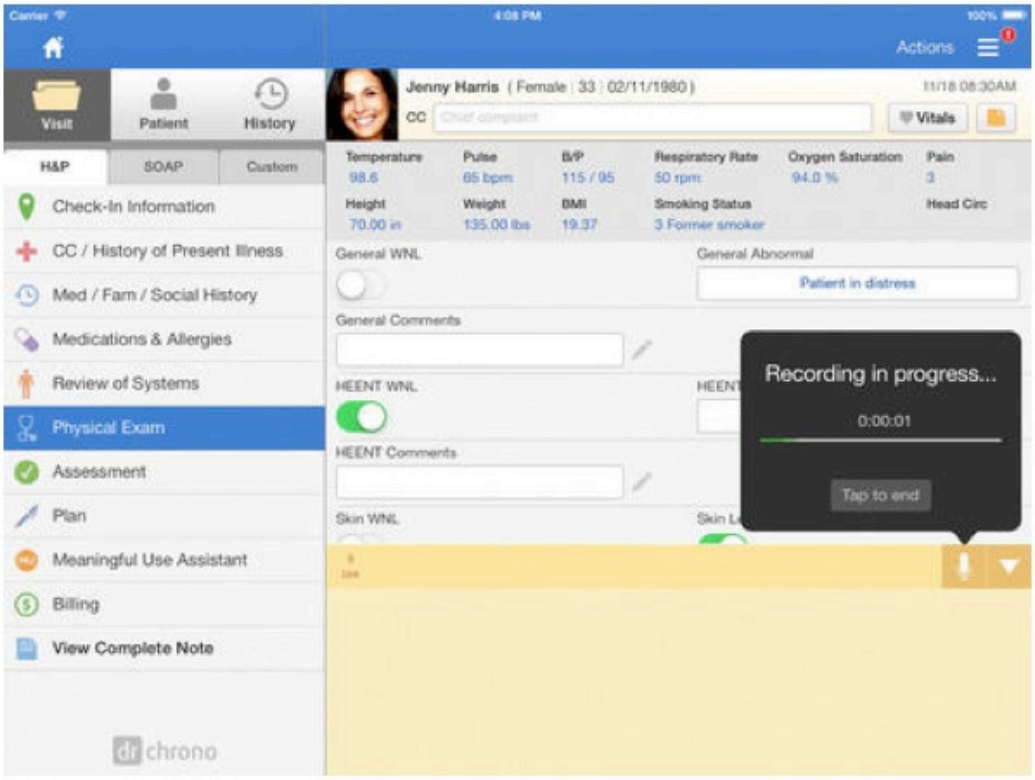

Figure 10. DrChrono Patient Information (from DrChrono, 2014).

c. Document Management Application: Google Drive

Google offers a file management service that combines document creation and editing functions with cloud-based synchronization and collaboration features (Duffy & Hachman, 2013). The Google Drive application allows multiple users to upload or create files in varying formats for storage, editing, and export. It allows

for many different users to be assigned varied levels of editing permissions and also permits several users to collaborate in real time. Finished documents can be exported in formats with which the user is accustomed to working, such as .doc, .ppt, and .pdf (Duffy & Hachman, 2013). A feature that sets Google Drive apart from other file-synchronization services is that it incorporates Optical Character Recognition (OCR) (Duffy & Hachman, 2013). OCR is an application's ability to recognize printed text (PC Magazine, 2014b). The Google Drive takes that technology a step further with its ability to extract text from images and .pdf documents (Duffy & Hachman, 2013). The universal nature of this application allows a wide variety of organizations to use Google's service, or one similar to it, including the military.

d. GPS and Navigation Application: Theodolite

Hunter Research and Technology has created a navigation application for the iOS called Theodolite. Combining many of the iPhone's existing features, Theodolite creates an augmented reality that captures, tags, and displays an array of useful information. Using the device's camera, GPS receiver, and accelerometers, this enhanced navigation application produces an electronic version of an actual theodolite instrument (see Figure 11) (University of Missouri-Columbia, 2011). Leveraging the smart aspects of the device, Hunter Research and Technology displays the user's position, altitude, bearing, attitude, and inclination. It can also calculate distances using rudimentary trigonometry, effectively functioning as a rangefinder. All of this information can be captured in a screenshot and geo-tagged for later use and even shared among specified users (see Figure 12). Even more advanced features such as data-logging, email export, mil-compass readout, optical and GPS attachments, and lens filters set Theodolite apart from normal navigation applications (Hunter Research and Technology, 2014). The military relevance to this application is clear. This technology represents many of the existing crossover applications that can be adapted for military use.

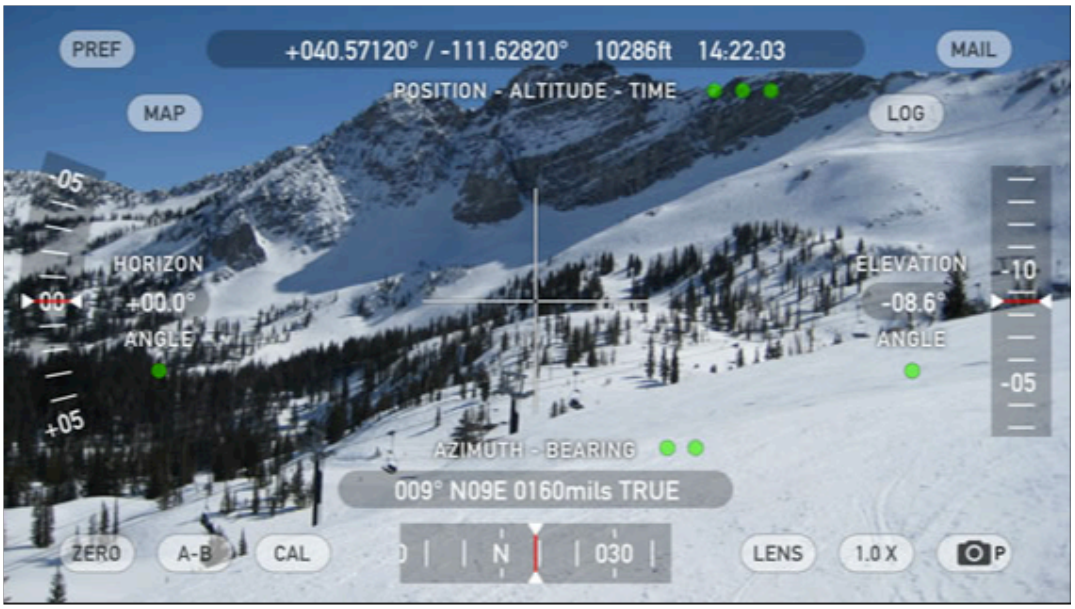

Figure 11. Theodolite Image Capture View
(from Hunter Research and Technology, 2014)

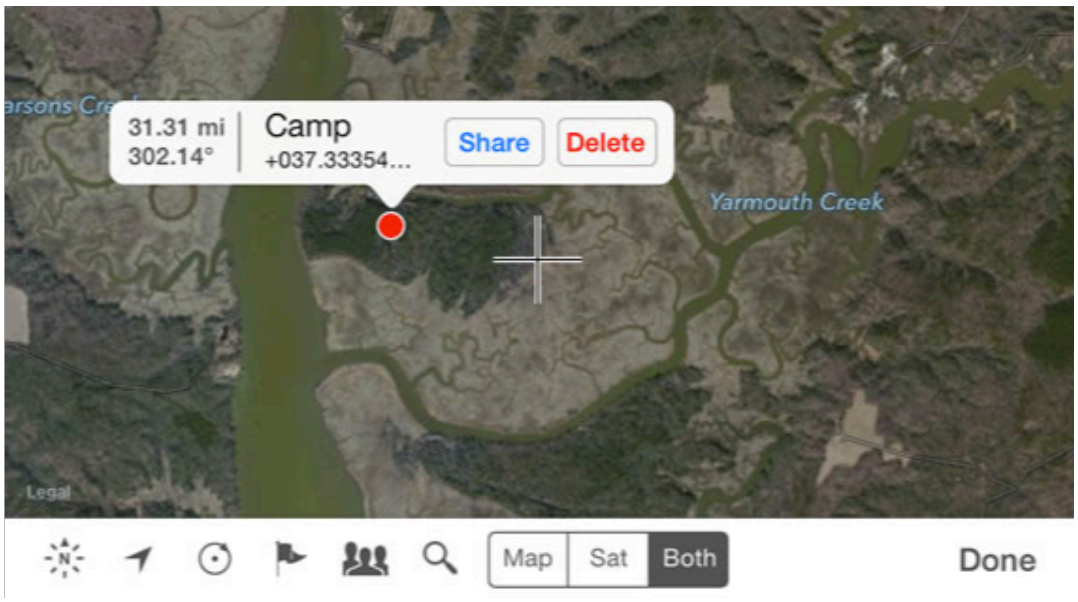

Figure 12. Theodolite Map View
(from Hunter Research and Technology, 2014)

4. Military Application Examples

While there are many mobile applications on the market such as Theodolite that have military utility, some applications have been developed

specifically for this reason. While these applications are not yet approved for official use, they demonstrate developers' initial platform progress while also exhibiting their awareness of the eventual integration of mobile devices within the military. USMC leadership has expressed the desire for smaller networked devices that not only contribute to the COP but can also provide enemy target location, distance, and direction to less experienced fire directors (Conway, 2008a). The following examples of mobile applications constitute that specific need as well as reveal a sample of the capabilities that a mobile device can provide to the individual Marine.

a. Fires Application: GUSTO, KILSWITCH, SafeStrike

Stauder Technologies has developed a target location and digital target handoff mobile application called GUSTO that enables Marines to conduct Digitally Aided Close Air Support (DACAS) and Call For Fire (CFF) missions with a smartphone (Phillips, 2013; StauderTechnologies, 2012). GUSTO is part of the Marine Corps' Target Location, Designation, and Handoff System (TLDHS) program (StauderTechnologies, 2012). The application leverages COTS Android smartphones as well as Stauder Technologies' Hyde device (see Figure 13) (Phillips, 2013). The Hyde Smart Hub provides connectivity between military devices such as radios, GPS devices, and laser rangefinders to mobile devices via encrypted wireless and Bluetooth communications (StauderTechnologies, 2014).

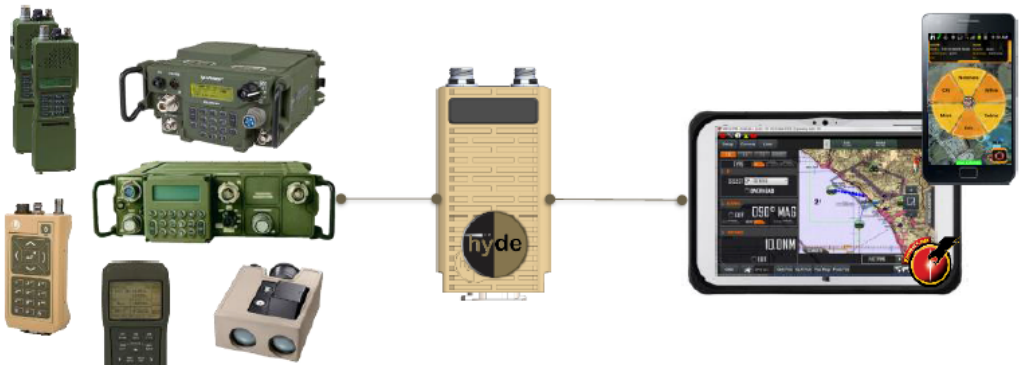

Figure 13. Stauder Technologies' Hyde 2.0 Smart Hub (from StauderTechnologies, 2014).

Another close air support (CAS) oriented application is the Naval Air System Command's Digital Precision Strike Suite (DPSS) developed Kinetic Integration Low-cost SoftWare Individual Tactical Combat Handheld (KILSWITCH) terminal (Barksdale, 2014). KILSWITCH enables Joint Terminal Attack Controllers (JTAC) to view extremely accurate gridded reference graphic (GRG) mensurated maps and video derived from the CAS aircraft (Pengelley, 2013). JTACs and other ground controllers can use the Android-based KILSWITCH application to select a target of interest on the ground. The selected target's location is sent to appropriately equipped aircraft and the pilot can direct aircraft's sensors onto the selected target. The pilot can then reply back to the JTAC with the aircrafts sensor-procured view of the target (Barksdale, 2014; Pengelley, 2013). KILSWITCH abbreviates the CAS communication timeline while introducing an additional measure of safety.

SafeStrike is yet another fires application developed by an Italian organization that accomplishes the same objectives as both GUSTO and KILSWITCH. SafeStrike is a map-based application that displays navigation and target information, 9-line and CFF scripts, danger-close and gun line overlays, as well as aircraft video (see Figure 14) (Rebel Alliance, 2014).

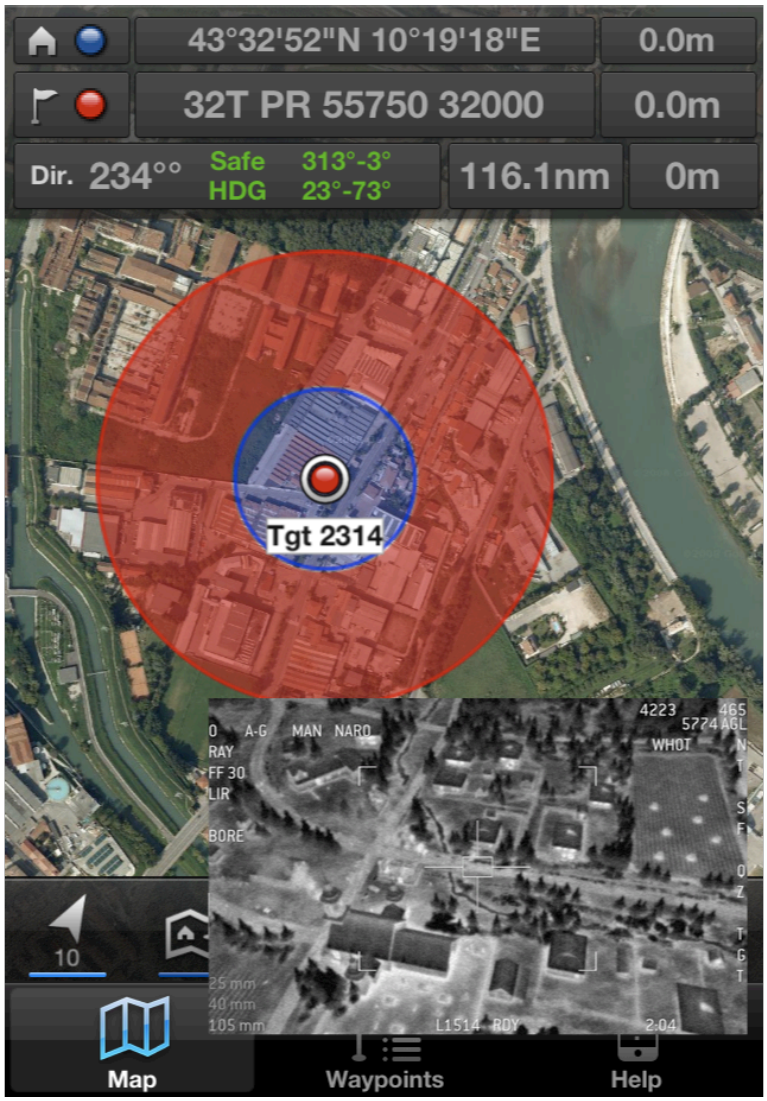

Figure 14. SafeStrike 3.1 Application (from Rebel Alliance, 2014)

b. Reporting Application: HELP

Many of the instances of communications exchange in military operations are briefs and reports that are standardized in format. The normalizing of these exchanges of information permits the development of reporting applications that can be employed in a large number of areas. The Handheld Emergency Logistics Program (HELP) application (see Figure 15) is one such program (Barnes, Bradley, Singh, & Das, 2014). Developed at the Naval Postgraduate School as part of student thesis work supported by HQMC Installations and Logistics (I&L),

HELP aids the warfighter in calling for assistance for casualty evacuations, emergency ordinance disposal requests, and rapid logistics requests (Barnes et al., 2014). Exploiting organic smartphone technologies, HELP assists in minimizing some of the errors associated with communicating in stressful situations (Barnes et al., 2014). HELP uses the smartphone's GPS receiver and menus, along with personalized settings to automatically fill in portions of the request (Barnes et al., 2014). HELP can then transmit the request to the appropriate agency or provide the user with a voice script to communicate the message via more conventional methods (Barnes et al., 2014). These types of reporting applications are essentially form-filled texts and can easily reduce the amount of errors in transmissions, increase response times, and allow untrained users to call for help during emergencies (Barnes et al., 2014).

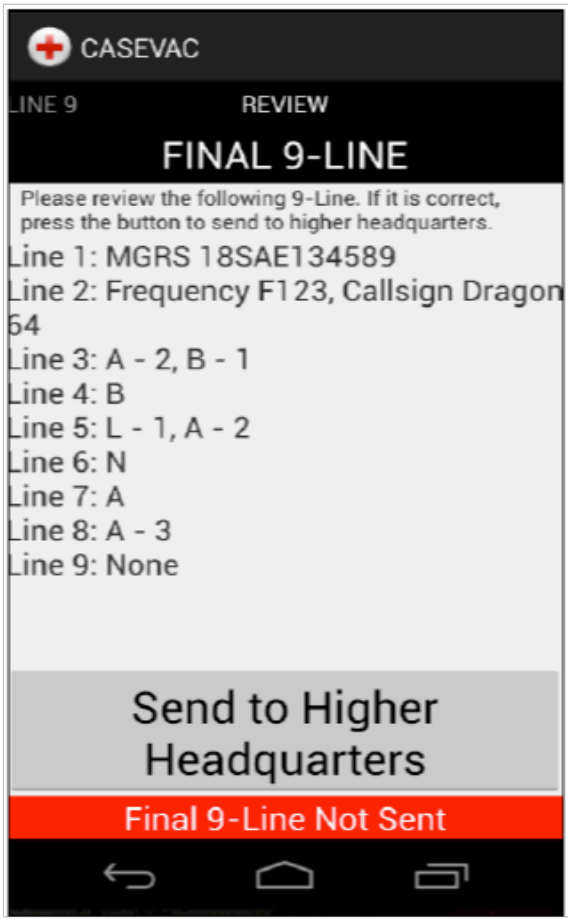

Figure 15. HELP Application (from Barnes et al., 2014)

c. Information Application: iCorps and Expeditionary Force 21

Another type of program that can be developed for military specific use is the information-based application. While this Mobile Information category is not military specific, it can be programmed to provide information that is aimed at a particular organization (Unhelkar & Murugesan, 2010). Two examples of this kind of application are the iCorps and United States Marine Corps Concepts and Programs (USMCCP) applications (Dunn, 2014; USMC, 2014c). The iCorps application displays categories of information and calculators that are useful to all Marines. The application contains orders and references, as well as information on vehicles, aircraft, and weapons that can be useful in a variety of circumstances (see Figure 16) (Dunn, 2014). The USMCCP application

accomplishes the same type of objective but is aimed at a different audience. This application was developed to convey the Marine Corps' strategic vision contained in Expeditionary Force 21 to individual Marines, planners, programmers, budgeteers, and industry (USMC, 2014c). The application breaks the document down in categorized content that is searchable and is rich in graphics that help to convey the Corps' message (USMC, 2014c). These types of Mobile Information applications are useful in communicating, storing, or retrieving a wide variety of information and data.

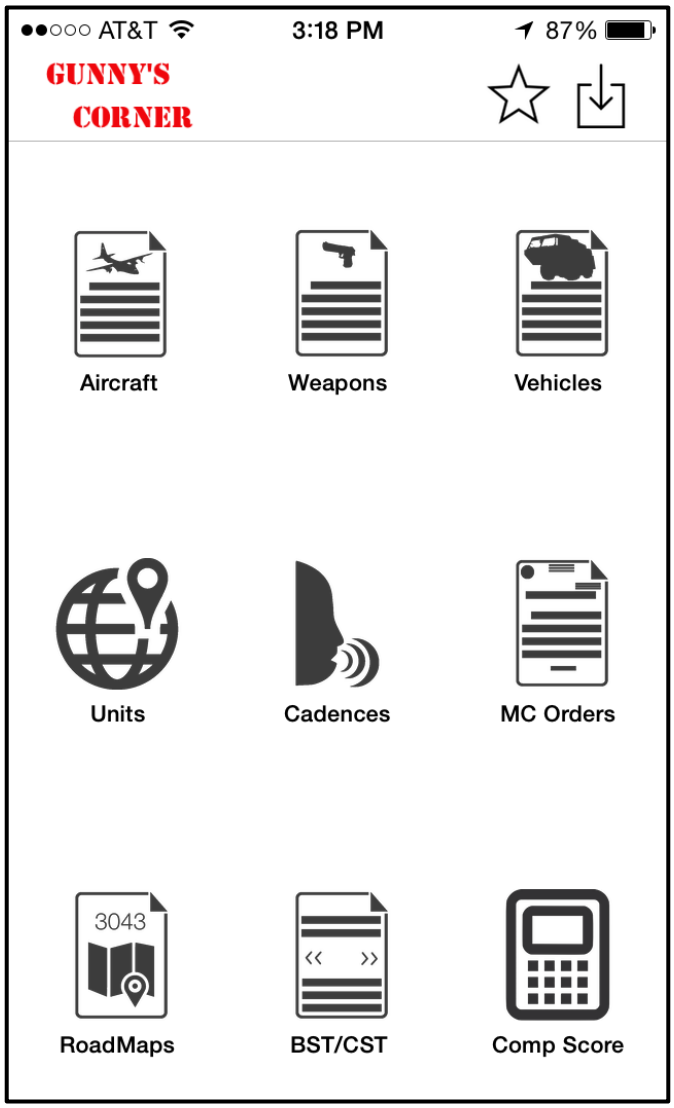

Figure 16. iCorps Pocket Reference Application (from Dunn, 2014)

B. CAPABILITIES DEVELOPMENT DIRECTORATE DATA

The Capabilities Development Directorate (CDD), within the Marine Corps' Combat Development and Integration (CD&I) branch, is an organization that "develops and integrates warfighting capabilities solutions that provide for an effective, integrated MAGTF capability, current and future, that anticipates strategic challenges and opportunities for the nation's defense" (Glueck, 2013). The CDD is the Marine Corps' planning effort to identify, budget for, and acquire future capabilities based on guidance such as Expeditionary Force 21 (Glueck, 2013). One of the CDD's products is a highly refined set of communication events, referred to as Information Exchange Requirements (IERs), that are essential to conveying information that is critical to mission success (Capabilities Development Directorate, 2012).

1. Information Exchange Requirements

The Information Exchange Requirements are the individual occasions in which an item of information is passed from one entity to another within a set of parameters. IERs have been identified and classified according to mission criticality across all three functional elements of the Marine Corps, as well as three specific defense planning scenarios (DPS) (Capabilities Development Directorate, 2012). The identification of the IERs has allowed a number of organizations to conduct planning and develop systems based upon IER criticality.

2. CDD Methods

The CDD first identified the IERs for the GCE in January of 2011 and then expanded their work to include the LCE and the ACE in June of the same year. The CDD first compiled inputs from a variety of sources including working groups, subject matter experts (SMEs), strategic guidance initiatives, manuals, after action reports (AARs), and standard operating procedures (SOPs). Next,

the IERs were vetted through a validation process that split the SMEs into groups by MAGTF element. The individual MAGTF SMEs reviewed the IERs and refined them by performer, format, and operating environment. The performer designated the sender and the receiver of the IER. The format indicated if the IER could be conveyed by voice, text, graphic, or video. The operating environment added additional fidelity by indicating if the IER was needed if the performer was in a fixed, static, or dismounted state. Now the CDD has a list of all occasions when a Marine or unit would need to communicate to another Marine or unit, broken down by MAGTF element, performer, message format, and mobility status (Capabilities Development Directorate, 2012).

Next, the CDD dispersed the SMEs into three groups to assess another element of the IER classification process. Three DPSs were introduced to give relevance to the IERs. The DPSs chosen were military engagement/power projection, crisis response, and small wars. The SMEs evaluated the IERs based on their experience and assigned values to each IER within a specific DPS. After this assessment was concluded, each IER was categorized by mission criticality and military operating environment. Finally, the IERs were organized and ranked into tiers according to mission criticality (Capabilities Development Directorate, 2012). The results and tiers are listed in Table 1.

Tier	Criteria	ACE	GCE	LCE
1	Mission Critical (MC) IERs validated for use in all scenarios and all environments.	43	32	11
2	MC IERs validated for use in at least one scenario and all environments.	24	58	59
3	MC and/or Non-Mission Critical (NMC) IERs validated for use in at least one scenario and one environment.	75	41	37
4	IERs validated for use but were not applicable in the scenario used or environment.	7	3	0
Total number of IERs per MAGTF element		149	134	107

Table 1. TIER Results (after Capbilities Development Directorate, 2012)

C. CHAPTER SUMMARY

Smartphones and applications were studied in this chapter. The varieties of technologies that are contained in the device were annotated and examples for their use were given. This led directly to the section on mobile applications. A developmental taxonomy was presented that organized applications into levels of capability and sophistication. A developmental framework that aids in the mobile application developmental challenges was also introduced.

A variety of civilian applications were presented and their capabilities were examined. These applications were chosen, not only for their potential military uses, but also because the organizations using these applications also deal with a high level of security risks and compliance regulations. Military specific applications were also introduced to indicate that developers are already preparing for the moment when the warfighter will take his or her smartphone with them to combat. Finally, the IERs from the CDD were presented and their method of derivation was reviewed. These IERs will form the basis from which the conclusions from this work will be achieved.

IV. INFORMATION EXCHANGE REQUIREMENTS ANALYSIS

This chapter further explores the Information Exchange Requirements (IERs) previously introduced. Evaluation criteria is defined and analysis is performed on the data obtained from the Capabilities Development Directorate (CDD) in order to map mobile application needs of the Marine Corps to essential Marine Air-Ground Task Force (MAGTF) communication events.

A. INTRODUCTION

Given the noted trends toward personal smartphone adoption and mobile business solutions, it is reasonable to deduce that the Marine Corps will place an increasing amount of emphasis on mobility, and mobile devices in particular. The Department of Defense's (DOD) Commercial Mobile Device Implementation Plan calls for the development and execution of a Mobile Application Store (Takai, 2013). This event signifies that the Marine Corps will need to develop and evaluate mobile applications. The research in this chapter identifies the types of applications for which the Marine Corps should place the most development emphasis. This analysis focuses on the utilitarian benefit of application types across the functional elements of the MAGTF with reference to the current IERs. Essentially, the Marine Corps may satisfy a large quantity of its most important warfighting information needs by focusing on the development of these particular types of mobile applications, potentially mitigating hardware device "lock-in."

B. METHODOLOGY

The IERs provided by the CDD proved to be a valuable source of information. However, this data did not provide substantial enough detail as to which of the 185 identified IERs would be applicable to more than one of the elements of the MAGTF. Once we identified the MAGTF's core IERs, we then screened them to determine if any of them would be potential candidates for

future application development. This screening process was accomplished through the use of a capability matrix.

C. REFINING THE DATA

Starting from the comprehensive collection of IERs, we processed the requirements to determine the IERs that may be used by multiple elements of the MAGTF during an operation. We distilled this data to produce a succinct list of Tier-1 IERs that were determined to be mission critical in all scenarios, in all environments, and for all three elements of the MAGTF. This list, as seen in Figure 17, was quite small.

Casualty Evacuation (CASEVAC) Request
Fragmentary Order (FRAG Order or FRAGO)
Medical Evacuation (MEDEVAC) Request
Rules of Engagement (ROE)
SALUTE Report
Search and Rescue Coordination Information

Figure 17. IERs common to all elements of the MAGTF

Due to the modest number of IERs in this list, we concluded that a larger list would be produced if we identified the IERs that were of Tier-1 status which were applicable to two of the three MAGTF elements. This approach is not unreasonable due to the frequency in which two of the three elements operate together. Using this method, we extracted a list of 23 IERs. They are identified in Figure 18 and explained in Appendix A.

5-Paragraph Order
9-Line Brief
Acknowledgment
Blue Force Information
Casualty Evacuation (CASEVAC) Request
Commander's Critical Information Requirements (CCIR)
Common Tactical Picture (CTP) data
Communications-Electronics Operating Instructions (CEOI)
Execution Checklist/ Matrix
Fragmentary Order (FRAG Order or FRAGO)
Ground Control Measures
Intelligence Report (INTREP)
Landing Zone (LZ) Brief
Maneuver Control Measures
Medical Evacuation (MEDEVAC) Request
Mission Card Information
Obstacle Report
Rules of Engagement (ROE)
SALUTE Report
Search and Rescue Coordination Information
Situation Report (SITREP)
Spot Report (SPOTREP)
Warning Order (WO)

Figure 18. IERs common to two of three MAGTF elements

D. IER TO APPLICATION SUPPORT MATRIX

We then created a matrix to evaluate whether or not these selected IERs would be viable candidates for further application consideration. Some of the IERs appear to be obvious subjects for mobile application feasibility. Others, based on a number of factors such as vehicle of information conveyance, media richness, and typical usage, may not produce the most effective applications for mobile device use. We created the IER-to-Application Support Matrix in order to evaluate all of the IERs on a consistent basis.

1. Support Matrix Decision Factors

The 23 Tier-1 IERs were considered against ten factors to determine if they would be suitable for mobile application development. The decision factors are not exhaustive and do not represent a formal level of evaluation. Rather, they present a common sense approach to validate the IERs for future use. These decision factors were

1. Demand
2. Presentation
3. Level of Change
4. Multi-Sensor Usage
5. Standardized Format
6. Complexity
7. System Redundancy
8. Mobility
9. Accuracy
10. Timeliness

Each IER decision factor (DF) was assigned a value from one to four based upon the level of applicability in each category. A higher value indicates more importance in that category. The totals of all of the categories indicate the IER's relative suitability to become a mobile application. The model allows for a weighted value for each of the decision factors such that the contribution of each individual factor to the composite score reflects the emphasis placed on each factor. The higher composite scores suggest that those IERs should be further researched for mobile application development. Assignment of values is based upon the following criteria:

1. DF may not contribute to IER's mobile application potential.
2. DF may slightly contribute to IER's mobile application potential.

3. DF may contribute to IER's mobile application potential.

4. DF may significantly contribute to IER's mobile application potential.

An explanation of the chosen decision factors provides the rationale for their inclusion into the matrix. The first measure, *Demand*, addresses whether or not the IER in question is significant enough to become an application on its own. The "Acknowledgment" and "Obstacle Report" IERs are simple events that are straightforward and do not warrant a separate mobile application to facilitate their accomplishment.

Presentation is the factor used to reflect how the information may be conveyed in the IER. In the most basic terms, mobile devices are capable of conveying information by voice, text, or graphical means. Values in the Presentation category were assigned based upon the level of media richness that the IER could deliver to the user in a mobile format. The use of a combination of conveyance formats could further enrich the user experience and enhance understanding of the information being communicated. For example, the SPOTREP IER has traditionally been relayed in the voice format via tactical radio. A SPOTREP mobile application could enhance the receiving party's comprehension of the report through the integration of maps, overlays, and icons, as well as textual information and even voice recordings. Higher values will be assigned to the IERs that can incorporate increasingly complex levels of media richness and information delivery.

Level of Change refers to the frequency at which the information being communicated is revised. Mobile devices are capable of sharing information that is continually evolving through the use of automatic or simplified reporting. The demand on the warfighter can be reduced when repeating tasks can be accomplished by a more accurate and automated mobile application. This factor will receive higher values if the communication event that it applies to needs frequent updating.

Multi-Sensor Usage is the degree to which the IER may leverage the use of organic mobile device sensors and tools. In addition to prominent attributes such as the screen, microphone and speaker(s), current mobile devices utilize built-in features that may be used in combination to create powerful mobile applications. The following collection is a non-exhaustive list of tools and sensors that are integrated into modern smartphones:

- Accelerometer
- Gyroscope
- Ambient light sensor
- Temperature and humidity sensors
- Barometer
- Magnetometer
- Pressure sensor

IERs that can integrate multiple sensors will be able to deliver more accurate and synoptic information and will correspondingly be assigned higher values within the decision matrix.

Standardized Format was included in the matrix because mobile applications are more easily developed when the information being communicated is presented in a commonly understood style. Despite this, the information presented in a standardized format may not necessarily be a favorable feature. The 5-Paragraph Order IER is a well-established format for the communication of orders. However, the 5-Paragraph Order's large size and tendency to be presented in a text format does not translate well into a useful mobile application. IERs that use commonly accepted formats were given higher matrix values to the extent that the standardized format can potentially add value to a mobile application.

In this matrix, *Complexity* is a measure of the intricate nature of the IER. Those IERs with increased complexity were given higher values than those that were simpler. Much like the *Demand* attribute, *Complexity* identifies and

helps to minimize the importance of those IERs that may be too simplistic to develop into a stand-alone application.

System Redundancy indicates whether or not the development of a particular IER into a mobile application would replace or provide redundancy to an existing system. Higher values were assigned to IERs that added redundancy. Similarly, *Mobility* places value on a potential application that permits access to information while on the move. Higher value is awarded if the prospective application delivers a user access to information that was previously inaccessible due to current systems' non-mobile status.

Accuracy is used as a decision factor to evaluate how the acute sensors that are organic to mobile devices could deliver and share information that is more accurate. In a similar manner, *Timeliness* measures how an IER-derived application might provide more timely information than more conventional methods of conveyance.

E. DECISION MATRIX RESULTS

Values were assigned to the decision matrix and ranked. The ranked values were divided into thirds to indicate the IERs that, according to this analysis, should be considered for mobile application development. Table 2 shows this final analysis.

	Demand	Presentation	Level of Change	Multi-Sensor Usage	Standardized Format	Complexity	System Redundancy	Mobility	Accuracy	Timeliness	Totals
Blue Force Information	4	4	4	4	2	4	4	4	4	4	38
Common Tactical Picture (CTP) data	4	4	4	4	2	4	4	4	4	4	38
Casualty Evacuation (CASEVAC) Request	4	4	3	4	4	3	2	3	4	4	35
Medical Evacuation (MEDEVAC) Request	4	4	3	3	4	3	2	4	4	4	35
Search and Rescue Coordination Information	4	4	3	4	4	2	2	4	4	4	35
9 Line Brief	3	3	2	4	4	3	4	2	4	4	33
Situation Report (SITREP)	2	3	4	3	4	2	2	4	4	3	31
SALUTE Report	2	3	3	3	4	2	2	3	3	4	29
Spot Report (SPOTREP)	2	3	4	3	3	2	2	4	3	3	29
Execution Checklist/ Matrix Dissemination	3	2	3	3	2	2	2	4	3	4	28
Landing Zone (LZ) Brief	2	3	1	3	4	2	2	3	3	4	27
Mission Card Information	3	2	2	3	3	2	2	3	3	3	26
5 Paragraph Order	3	2	2	2	2	3	4	3	1	2	24
Warning Order (WO)	3	2	2	2	2	2	2	3	3	2	23
Communications-Electronics Operating Instructions (CEOI)	3	2	1	2	3	2	2	3	2	2	22
Ground Control Measures	2	3	1	2	3	2	2	3	2	2	22
Intelligence Report (INTREP)	2	3	1	2	2	3	2	3	1	3	22
Maneuver Control Measures	2	3	1	2	2	2	2	3	2	3	22
Fragmentary Order	3	2	2	2	2	2	2	2	2	2	21
Obstacle Report	2	3	1	2	2	2	2	3	2	2	21
Acknowledgment	1	1	1	2	4	1	2	2	1	3	18
Commander's Critical Information Requirements (CCIR)	2	2	1	2	2	2	2	2	1	2	18
Rules of Engagement (ROE)	2	2	1	2	2	2	2	2	1	1	17

Table 2. IER Final Analysis

The IER analysis produced a relatively even stratification of Tier-1 communication events. Most of the highest ranked IERs were obvious candidates for future development based upon the criticality and complexity of the associated task and the added benefits that mobile device sensors can provide. These IERs were associated with tools such as position location and reporting, GPS map overlays, and timely delivery of information. Mid-level IERs mainly consisted of communication events that involved routine reporting of data or situations that were of importance but not of significant priority. These types of IERs could benefit from an application or group of applications that involved fields and drop-down menus that are filled out and delivered in a manner that is consistent with most standard formats. As such, the user would benefit from the efficiency of using pre-formatted constructs. The lowest ranked IERs do not

reflect situations in which a stand-alone application is warranted. These events could be included with other applications but should not be the focus of future mobile application development.

1. Top Ranked IERs

Six IERs comprised the group that showed the most potential for developmental consideration. These IERs were

1. Blue Force Information
2. CTP Data
3. CASEVAC Request
4. MEDEVAC Request
5. SAR Coordination Information
6. 9-Line Brief

Considering that CTP Data incorporates Blue Force information, the two IERs should be considered as one. Similarly, CASEVAC and MEDEVAC requests, while different, essentially require the same information for processing and execution. Therefore, these two IERs should also be considered as one. This list of four IERs should be considered as the top recommendations for future mobile application development or refinement.

a. Common Tactical Picture Application

A CTP application could leverage automatic position reporting to provide individual, real-time battlefield SA and common operational picture (COP) information to those who need it. According to Cahlink (2004), the purpose of CTP information is to reduce the likelihood of fratricide by providing the "ability to pinpoint the whereabouts of friendly forces in a rapidly changing battle-space" (p. 66). Like current Blue Force Tracker (BFT) systems in use today, a mobile application would, at a minimum, provide one-way position, location, and identification (PLI) data (Stengrim, 2005). Combined with map overlays and unit

data, such as identification, weapons capabilities, and communication details, and effective presentation and processing of this information could produce a very powerful application with tremendous influence on the area of operations.

b. CASEVAC/MEDEVAC Application

A CASEVAC/MEDEVAC application could be a very useful tool for the timely delivery of information that is critical in getting injured warfighters the help that they need. The integration of PLI data and standardized formatting could help to increase the speed and accuracy with which these requests are conveyed. Dropdown menus and large data entry options can also increase the timely precision that is often required but difficult to achieve by conventional means such as tactical radio because of the level of anxiety that is inherent in the situation. The receipt of this vital information could also be enhanced through the use of an application. The ability to actually see, review, and accurately forward a request is greatly enhanced over traditional means such as tactical radio. Barnes and Bradley (2014) have created the HELP application (Figure 15) that stands as an example of what such an application may look like. Inclusion of imaging from the smartphone camera could also provide useful triage information to expedite processing of the victims. The leveraging of a smart device's built-in features and a modern warfighter's familiarity could very well save lives through timely and accurate reporting of critical information.

c. SAR Application

SAR communications are the most important, but too frequently, the weakest link in SAR operations (National Search and Rescue Committee, 2000). Mobile devices have the potential to add to and supplement the number of tools that are available to personnel in distress. Alerting, identification friend or foe (IFF), updated PLI, and textual communication are capabilities that could be offered by a mobile device. The ability to automatically update mobile devices could also allow survivors to access up-to-date essential data for use through other communications means. For example, an updated application could include

a frequency changeover list, authentication tables, and code words that could be used with more conventional communication methods. Security concerns and additional SAR best practices would need to be addressed and included in the development of the application to help protect the isolated personnel against hostile exploitation of the mobile device.

d. CAS Application

Close Air Support (CAS) is an important part of maneuver warfare and a fundamental mission for those engaged with enemy combatants. CAS is a difficult and complex mission to execute that is, like CASEVAC and MEDEVAC operations, compounded by the urgent and often desperate demands of the situation. As mentioned with the previous applications, a CAS application could leverage a smart device's capabilities to reduce the demand placed on the users and deliver a more accurate and timely communication exchange that provides a much more media rich communication exchange for all associated with the mission. Rebel Alliance's Safe Strike (2014) (Figure 14) is but one example of this type of application. The CAS mission is a highly intricate operation that requires very accurate and timely information exchanges. The automation of portions of this process can help deliver expedient fires for Marines in urgent combat situations.

2. Mid-level IERs

The IERs that were ranked in this category represent the type of communication exchanges that are routine and important but not as time-critical as the previous IERs. This category contains a number of reports, such as the SPOTREP, SITREP, SALUTE, and Mission Card. These constitute what could be identified as a type of reporting application. Within one application, a number of different reports could be generated. Using dropdown menus and following standard formatting, these reports could be easily produced and forwarded to one or any number of agencies or recipients at once.

The execution checklist is essentially a simplified format for reporting events. Mission information could be preloaded into the application before an operation and reporting could be as easy as selecting an event and confirming its accomplishment. If the event is location driven, the report could possibly be sent automatically using PLI data within the device.

The LZ Brief presents an additional type of application that is needed. The LZ Brief is standard and required across the MAGTF; however, it is actually used so infrequently its contents may be easily forgotten. While the LZ Brief itself does not warrant its own application, it could be contained in a type of reference application. Similar to the type developed by iCorps (Figure 16), this application could include a myriad of information that could be referenced at a moment's notice.

3. Low-level IERs

The lower-level IERs are events that do not warrant further consideration for mobile application development. These IERs are better conveyed through more conventional systems, within other applications, or through textual means such as email.

a. Warning, 5 Paragraph, and Fragmentary Orders

The orders process may be better conveyed through other means than a mobile application. The warning and fragmentary orders are typically conveyed through verbal communications. The operations order is generally too lengthy to be delivered by any means other than textual. The order delivery process should not be considered for specific application development that is not already addressed with existing organic mobile device applications.

b. Communications-Electronics Operating Instructions

The Communications-Electronics Operating Instructions is a collection of orders, instructions, and data used to guide communications protocols. The

CEOI contains information such as unit call-signs, cryptographic and frequency changeover times, and authentication procedures, etc. This information is vital and is frequently updated, making it a viable candidate for inclusion within a reference application.

c. Ground Control Measures, Maneuver Control Measures and Obstacle Report

The Ground and Maneuver Control Measures and Obstacle Report are C2 tools used to coordinate operations within a specified area. These measures would normally be found in other systems associated with Operations Centers. Their use may be considered for inclusion within COP data.

d. Intelligence Report

While the Intelligence Report is a vital piece of information, it does not need to be developed into an individual application. The INTREP could be better conveyed through email.

e. Acknowledgment

The Acknowledgement is technically an identified IER that fell within all of the parameters that were designed for the conduct of this research. This IER is a simple confirmation that a particular piece of information has been received. Its simplistic nature excludes it from further development as an application but will inevitably be included in a multitude of other mobile applications.

F. CHAPTER CONCLUSION

Chapter IV introduced the information exchange requirement data and the analytical process that we applied to it. Our methodologies allowed us to distill the IERs into a select number that would provide the most benefit to the widest category of Marines, whether they belong to the air, ground, or logistics element of the MAGTF. Those selected IERs were then evaluated against a set of criteria that further categorized the IERs and ranked them according to their potential to be further developed into a mobile application. The best candidates such as CTP

data, life-saving MEDEVAC requests, and fire control aides, have emerged as candidates that could potentially have a large impact on some of the ways in which the Marine Corps conducts its business.

V. CONCLUSION

A. REVIEW

This research stems from the assumption that mobile devices will become more and more prevalent within garrison and deployed environments. Considering this and the DOD's implementation of a mobile application store, it can be further deduced that mobile device applications will need to be developed for use in these environments. This research ties the future needs of the Marine Corps with current, documented Company-level communication events that are applicable to all three functional elements of the MAGTF in a number of deployment scenarios. Comparing IERs that were developed and approved by the CDD against an original decision support matrix produced a number of IERs that should be the focus of initial mobile application production. These are the IERs that could benefit the widest contingent of Marines.

B. CONCLUSION

A number of IERs were analyzed and recommended for future development and use within the Marine Air-Ground Task Force. The most pressing mobile device application requirement appears to be associated with time-critical events that have an additional accuracy component. Other needs are related battlefield situational awareness and command and control improvements. Other types of mobile applications that will need to be advanced include reporting and reference applications. The use and integration of mobile smart devices is growing daily. Mobile device integration into MAGTF operations appears to be inevitable. With the ability to offer solutions to the most common and pressing communication events, the Marine Corps should consider the identified IERs for future development into practical and potentially life-saving mobile device applications.

C. RECOMMENDATIONS FOR FURTHER RESEARCH

Much work needs to be done to further the effort to deliver wireless communication capabilities down to the individual level. Within the scope of this research, a set of requirements needs to be generated for each of the recommended applications. Each mobile device application that is recommended for future development will need to be researched in areas such as capability, capacity, ease of use, conformity to existing regulations, policies, and procedures, among other areas of consideration. Beyond this, additional aspects that were largely ignored in this research for the sake of focus need to be addressed. The two most apparent of these aspects are security and connectivity.

LIST OF REFERENCES

Amos, J. (2010). *35th Commandant of the Marine Corps, Commandant's planning guidance*. Washington, DC: United States Marine Corps.

Amos, J. (2012). *2012 Report to the house armed services committee on the posture of the United States Marine Corps*. Washington, DC: United States Marine Corps.

Aruba Networks. (2014). Onboard, secure and manage thousands of devices. Retrieved from http://www.arubanetworks.com/products/clearpass/device-management/

Barksdale, T. (2014, July). KILSWITCH and the way ahead. *Marine Corps Gazette*, 34–37. Retrieved from https://www.mca-marines.org/gazette/2014/07/cas

Barnes, M., Bradley, C., Singh, G., & Das, A. (2014). HELP: Handheld Emergency Logistics Program for generating structured requests in stressful conditions. *Procedia Engineering*, (September). Retrieved from http://www.sciencedirect.com/science/article/pii/S1877705814010236

Bernhart-Walker, M. (2014). DOD's MDM, app store to support 100,000 users by September. Retrieved from http://www.fiercemobilegovernment.com/story/dods-mdm-app-store-support-100000-users-september/2014-01-28

Bluetooth. (2014). What is bluetooth technology? Retrieved September 24, 2014, from http://www.bluetooth.com/Pages/what-is-bluetooth-technology.aspx

Brown-Willson Group. (2014). *Top 20 virtualized & native iPad EHR applications, ambulatory & inpatient support tools*. Clearwater, FL: Black Book Rankings.

Cahlink, G. (2004, June). Better "blue force" tracking. *Air Force Magazine*, 66–69.

Capbilities Development Directorate. (2012). *MAGTF information exchange requirements for the company level and below*. Quantico, VA: Capabilities Development Directorate.

Carter, J. (2013). What is NFC and why is it in your phone? Retrieved September 24, 2014, from http://www.techradar.com/us/news/phone-and-communications/what-is-nfc-and-why-is-it-in-your-phone-948410

CIO Council. (2012a). *Digital government: Building a 21st century platform to better serve the American people*. Washington, DC: Author. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Digital+Government:+Building+a+21st+Century+Platform+to+Better+Serve+the+American+People#0

CIO Council. (2012b). *Government use of mobile technology*. Washington, DC: Author.

Conway, J. (2006). *Renaming of the Combat Service Support Element (CSSE) to the Logistics Combat Element (LCE).* Washington, DC: United States Marine Corps.

Conway, J. (2008a). *A Concept for enhanced company operations.* Washington, DC: United States Marine Corps.

Conway, J. (2008b). *Marine Corps vision & strategy 2025*. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA519807

Dempsey, M. (2012). *Capstone concept for joint operations: Joint force 2020.* Washington, DC: Joint Chiefs of Staff. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Capstone+Concept+for+Joint+Operations+:+Joint+Force+2020#0

DISA. (2013). *DISA's Commercial mobile device implementation plan phased timeline*. Fort Meade, MD.

Dixon, J. (Marine C. S. C. (2012). *Technology development strategy for handheld command and control*. Quantico, VA: Marine Corps Systems Command

DOD. (2002). J*oint doctrine for targeting*. Washington, DC: Author.

DOD. (2014). *Department of defense dictionary of military and associated Terms.* Washington, DC: Author. Retrieved from http://www.fpa.org/usr_doc/38112.pdf

Downs, A., Fronczek, L., Morse, E., Weiss, B., Bashor, I., & Schlenoff, C. (2014). *Performance testing and evaluation of transformative apps devices*. *ITEA Journal*, *35*(1), 58–64.

DrChrono. (2014). DrChrono mobile application Retrieved August 10, 2014, from www.drchrono.com

Duffy, J., & Hachman, M. (2013). *Google drive review and rating*. Retrieved October 15, 2014, from http://www.pcmag.com/article2/0,2817,2403546,00.asp

Dunn, A. (2014). iCorps online mobile application. Retrieved October 19, 2014, from http://www.sciencedirect.com/science/article/pii/S1877705814010236

Eldridge, E. (2013). *Marine Corps operating concept for information operations*, (February). Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA578793

Ericom. (2012). *BYOD here to stay, but organizations must adapt*. Closter, NJ: Author.

Extreme Networks. (2014). *Bringing order to the chaos of "bring your own device."* Retrieved from http://www.extremenetworks.com/resources/bringing-order-to-the-chaos-a-byod-white-paper/

FindTheBest. (2014). *Best smartphones comparison 2014 - Reviews and ratings*. Retrieved September 24, 2014, from http://smartphones.findthebest.com/

ForeFlight. (2014). Foreflight mobile app. Retrieved August 12, 2014, from https://www.foreflight.com/ipad/

Futuremark. (2014). *Futuremark hardware channel - Mobile devices, graphics card, processor, motherboard reviews.* Retrieved September 24, 2014, from http://www.futuremark.com/hardware/

Gafni, R., & Geri, N. (2013). Generation Y versus generation X: Differences in smartphone adaptation. *Learning in the Technological Era: Proceedings of the …*, 18–23. Retrieved from http://www.openu.ac.il/innovation/chais2013/download/b1_4.pdf

Glueck, K. (2013). MCCDC & CD&I command brief. Quantico, VA: United States Marine Corps. Retrieved from http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CCAQFjAA&url=http://www.mccdc.marines.mil/Portals/172/Docs/MCCDC/Command%20Briefs/MCCDC%20CDI%20Command%20Brief%20Website%20Oct%202013.pdf&ei=7HJEVOWCHeuIi

Good Technology. (2011). *Good Technology state of BYOD report*. Sunnyvale, CA: Author.

Gunelius, S. (2014). *Mobile devices to surpass the number of people on earth*. Retrieved August 6, 2015, from http://aci.info/2014/05/03/mobile-devices-to-surpass-the-number-of-people-on-earth-infographic/

Hunter Research and Technology. (2014). Theodolite iPhone app. Retrieved October 15, 2014, from http://hunter.pairsite.com/theodolite/

Mercado, J. E., & Murphy, J. S. (2011). *Evaluating mobile device usage in the Army*. Fort Benning, GA: U.S. Army Research Institute.

Nadel, B. (2014). Wi-Fi tethering 101: *Use a smartphone as a mobile hotspot* | Computerworld. Retrieved September 24, 2014, from http://www.computerworld.com/article/2499772/mobile-wireless/wi-fi-tethering-101-use-a-smartphone-as-a-mobile-hotspot.html

Nah, F., Siau, K., & Sheng, H. (2005). The value of mobile applications: A utility company study. *Communications of the ACM*, *48*(2), 85–90. Retrieved from http://dl.acm.org/citation.cfm?id=1042095

Nally, K. (2010). *Marine Corps information enterprise (MCIENT) strategy*. *… from United States Marine Corps website: Http://www. …*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Marine+Corps+Information+Enterprise+(MCIENT)+Strategy#0

National Search and Rescue Committee. (2000). *United States national search and rescue supplement to the international aeronautical and maritime search and rescue manual*. Washington, DC: Author.

Parsons, D. (2012). Pentagon struggles to integrate smartphones, create mobile workforce. *National Defense*. Retrieved from http://www.questia.com/magazine/1G1-302664199/pentagon-struggles-to-integrate-smartphones-create

PC Magazine. (2014). OCR definition from PC magazine encyclopedia. Retrieved October 15, 2014, from http://www.pcmag.com/encyclopedia/term/48267/ocr

Pearlson, K., & Saunders, C. (2012). *Managing and using informations systems* (Fifth.). Hoboken, NJ: John Wiley & Sons.

Pengelley, R. (2013). RIPN opens new avenues for ROVER in the air and on the ground*. International Defense Review*. Retrieved from https://janes.ihs.com.libproxy.nps.edu/CustomPages/Janes/DisplayPage.aspx?DocType=News&ItemId=+++1595211&Pubabbrev=IDR

Perez, S. (2014). *iTunes app store now has 1.2 million apps, has seen 75 billion downloads to date.* Retrieved October 13, 2014, from

http://techcrunch.com/2014/06/02/itunes-app-store-now-has-1-2-million-apps-has-seen-75-billion-downloads-to-date/

Phillips, M. (2013, June). Air-to-ground and ground-to-air communications: Digitally aided close air support. *Military Technology*, 66–69. Bonn, Germany: Monch Publishing Group.

Rebel Alliance. (2014). Safe Strike app by Rebel Alliance S.r.l. Retrieved October 19, 2014, from http://www.safestrike.it/index.php

Smith, A. (2013). Smartphone ownership – 2013 update. *Pew Research Center: Washington, D.C.,* Retrieved from http://pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx

Starbucks. (2015). Starbucks App for iPhone, Starbucks Coffee Company. Retrieved September 18, 2015, from http://www.starbucks.com/coffeehouse/mobile-apps/mystarbucks

StauderTechnologies. (2012). *Stauder Technologies delivers first digital targeting handoff Android app to U.S. Marine Corps*. Retrieved October 16, 2014, from file:///Users/JesseAdkison/Documents/School/Thesis/Apps/Military Apps/Stauder Technologies - Gusto News

StauderTechnologies. (2014). *Hyde 2.0 multi-use tactical communications smart hub.* St. Peters, MO: Stauder Technologies.

Stengrim, D. (2005). *Blue on blue: Tracking blue forces across the MAGTF*. Quantico, VA: United States Marine Corps Command and Staff College.

Takai, T. (2013). *Department of Defense commercial mobile device implementation plan*. Washington, DC: Author.

TechTerms. (2014). The tech terms computer dictionary. Retrieved September 24, 2014, from http://www.techterms.com/

TheAppMagazine. (2014). *DrChrono EHR medical app review – iPad.* Retrieved October 14, 2014, from http://theappmagazine.com/drchrono-ehr-medical-app-review-ipad/

Unhelkar, B., & Murugesan, S. (2010). The enterprise mobile applications development framework. *IT Professional*, *12*(3), 33–40. Retrieved from http://doi.ieeecomputersociety.org/10.1109/MITP.2010.45

University of Missouri-Columbia. (2011). MU engineers developing military applications for smartphones. *NewsRx Health & Science*, (July), 83.

USMC. (1940). *Small wars manual*. Washington, DC: Author. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA421035

USMC. (1996). *Marine Corps doctrinal publication 6: Command and control.* Washington, DC: Author.

USMC. (1998). *Organization of Marine Corps forces*. Washington, DC: United States Marine Corps. Retrieved from http://www.navybmr.com/study material 3/MCRP 5–12D.pdf

USMC. (2010). *Marine Corps operating concepts,* 165. Washington, DC: Author.

USMC. (2012). *The Marine Corps " A young and vigorous force " demographics update December 2012*. Quantico, VA. Retrieved from http://www.usmc-mccs.org/buspartners/sponsorship_demographics.cfm?sid=mccs&smid=6&ssmid=1

USMC. (2013a). *Marine Corps commercial mobile device strategy*. Washington, DC: Author.

USMC. (2013b). *United States Marine Corps command and control roadmap*. Quantico, VA: Author.

USMC. (2014a). 31st Marine Expeditionary Unit. Retrieved August 25, 2014, from http://www.31stmeu.marines.mil/

USMC. (2014b). *Expeditionary force 21*. Washington, DC: Author.

USMC. (2014c). USMCCP mobile application. Retrieved October 20, 2014, from https://itunes.apple.com/us/app/usmccp/id814053840?ls=1&mt=8

Wallin, L. (2011). *Gartner's view on "bring your own" in client computing*. Stamford, CT: Gartner.

Zachman International. (2014). Zachman framework. Retrieved October 12, 2014, from https://www.zachman.com/about-the-zachman-framework

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California